Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP04/019110

International filing date: 21 December 2004 (21.12.2004)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2003-433903
Filing date: 26 December 2003 (26.12.2003)

Date of receipt at the International Bureau: 17 February 2005 (17.02.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

24.12.2004

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年１２月２６日

出願番号
Application Number: 特願２００３－４３３９０３

[ST. 10/C]: ［ＪＰ２００３－４３３９０３］

出願人
Applicant(s): 松下電器産業株式会社

２００５年　２月　４日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号　出証特２００５－３００６７８４

【書類名】　特許願
【整理番号】　2048150070
【提出日】　平成15年12月26日
【あて先】　特許庁長官　殿
【国際特許分類】　G09C　5/00
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　布田　裕一
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　大森　基司
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100090446
　【弁理士】
　【氏名又は名称】　中島　司朗
【手数料の表示】
　【予納台帳番号】　014823
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9003742

【書類名】特許請求の範囲
【請求項１】
鍵発行サーバと、端末装置を備え、前記鍵発行サーバから素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行システムであって、
前記鍵発行サーバは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成部と、を備え、
前記端末装置は、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵を格納する公開鍵格納部と、を備え、
前記素数生成部は、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて前記素数を生成すること
を特徴とする鍵発行システム。
【請求項２】
鍵発行サーバと、証明書発行サーバと、端末装置を備え、前記鍵発行サーバが素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を生成し、前記証明書発行サーバが前記公開鍵に対する公開鍵証明書を生成し、前記鍵発行サーバが前記秘密鍵及び公開鍵証明書を前記端末装置へ送信する鍵発行システムであって、
前記鍵発行サーバは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成部と、を備え、
前記証明書発行サーバは、前記公開鍵に対する前記公開鍵証明書を生成する公開鍵証明書生成部を備え、
前記端末装置は、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵証明書を格納する公開鍵証明書格納部と、を備え、
前記素数生成部は、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて前記素数を生成すること
を特徴とする鍵発行システム。
【請求項３】
前記証明書発行サーバは、さらに、前記公開鍵が前記発行識別子に基づいた前記素数を用いて生成されているかを判定する鍵判定部を備えること
を特徴とする請求項２記載の鍵発行システム。
【請求項４】
前記素数生成部は、第１素数ｑ、乱数Ｒ、前記発行識別子情報ＩＤＩ及び、前記発行識別子情報ＩＤＩと乱数Ｒから整数を生成する単射関数ｆを用いてＮ＝２×ｆ（ＩＤＩ，Ｒ）×ｑ＋１で表される素数Ｎを生成すること
を特徴とする請求項１から請求項３のいずれか１項に記載の鍵発行システム。
【請求項５】
前記素数生成部は、ｌｅｎビットの素数を生成し、
ｌｅｎｑ≧ｌｅｎ／２を満たすｌｅｎｑビットの第１の素数ｑを生成する素数情報生成手段と、
乱数Ｒを生成する乱数生成手段と、
前記発行識別子情報ＩＤＩ、前記第１の素数ｑ、前記乱数Ｒ及び、前記発行識別子情報ＩＤＩと乱数Ｒから整数を生成する単射関数ｆを用いてＮ＝２×ｆ（ＩＤＩ，Ｒ）×ｑ＋１で表される素数候補Ｎを生成する素数候補生成部と、
前記素数候補Ｎに対し、２＾（Ｎ－１）＝１　ｍｏｄ　Ｎを満たすか否かを判定する第１の素数判定部と、
前記素数候補Ｎ及び前記乱数Ｒに対し、２＾（２Ｒ）　≠　１　ｍｏｄ　Ｎを満たすか否かを判定する第２の素数判定部と、を備えること
を特徴とする請求項１から請求項３のいずれか１項に記載の鍵発行システム（ここで、

ａ＾ｘはａのｘ乗を示す）。
【請求項６】
前記素数生成部は、ｌｅｎビットの素数を生成し、
ｌｅｎｑ≧ｌｅｎ／２を満たすｌｅｎｑビットの第１の素数ｑを生成する素数情報生成手段と、
乱数Ｒを生成する乱数生成手段と、
前記発行識別子情報ＩＤＩ、前記第１の素数ｑ、前記乱数Ｒ及び、前記発行識別子情報ＩＤＩと乱数Ｒから整数を生成する単射関数ｆを用いてＮ＝２×ｆ（ＩＤＩ，Ｒ）×ｑ＋１で表される素数候補Ｎを生成する素数候補生成部と、
前記素数候補Ｎに対し、２＾（Ｎ－１）＝１　ｍｏｄ　Ｎを満たすか否かを判定する第１の素数判定部と、
前記素数候補Ｎ及び前記乱数Ｒに対し、ＧＣＤ（２＾（２Ｒ）－１，Ｎ）＝１を満たすか否かを判定する第２の素数判定部と、を備えること
を特徴とする請求項１から請求項３のいずれか１項に記載の鍵発行システム。
【請求項７】
前記発行識別子情報は、鍵発行サーバを識別する鍵発行サーバ識別子を含むこと
を特徴とする請求項１から請求項６のいずれか１項に記載の鍵発行システム。
【請求項８】
前記単射関数ｆは、前記発行識別子情報ＩＤＩと前記乱数Ｒを用いて、ｆ（ＩＤＩ，Ｒ）＝ＩＤＩ｜｜Ｒであること
を特徴とする請求項１から７記載の鍵発行システム（ここで、ａ||ｘはａとｘの連結を示す）。
【請求項９】
鍵発行サーバと、端末装置を備え、前記鍵発行サーバから素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行システムにおける端末装置であって、
前記端末装置は、素数を含む前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵を格納する公開鍵格納部と、を備え、
前記秘密鍵は発行識別子情報に基づいて生成された素数を含み、
前記素数は、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて生成されていること
を特徴とする端末装置。
【請求項１０】
鍵発行サーバと、証明書発行サーバと、端末装置を備え、前記鍵発行サーバが素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を生成し、前記証明書発行サーバが前記公開鍵に対する公開鍵証明書を生成し、前記鍵発行サーバが前記秘密鍵及び公開鍵証明書を前記端末装置へ送信する鍵発行システムにおける端末装置であって、
前記端末装置は、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵証明書を格納する公開鍵証明書格納部と、を備え、
前記秘密鍵は発行識別子情報ＩＤＩに基づいて生成された素数を含み、
前記素数は、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて生成されていること
を特徴とする端末装置。
【請求項１１】
前記素数は、第１素数ｑ、乱数Ｒ、前記発行識別子情報ＩＤＩ及び、前記発行識別子情報ＩＤＩと乱数Ｒから整数を生成する単射関数ｆを用いてＮ＝２×ｆ（ＩＤＩ，Ｒ）×ｑ＋１で表されること
を特徴とする請求項９または請求項１０記載の端末装置。
【請求項１２】
前記単射関数ｆは、前記発行識別子情報ＩＤＩと前記乱数Ｒを用いて、ｆ（ＩＤＩ，Ｒ

）＝ＩＤＩ｜｜Ｒであること
を特徴とする請求項９から請求項１１のいずれか１項に記載の端末装置。
【請求項１３】
鍵発行サーバと、端末装置を備え、前記鍵発行サーバから素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行システムにおける鍵発行サーバであって、
前記鍵発行サーバは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成部と、を備え、
前記素数生成部は、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて前記素数を生成すること
を特徴とする鍵発行サーバ。
【請求項１４】
前記素数生成部は、第１素数ｑ、乱数Ｒ、前記発行識別子情報ＩＤＩ及び、前記発行識別子情報ＩＤＩと乱数Ｒから整数を生成する単射関数ｆを用いてＮ＝２×ｆ（ＩＤＩ，Ｒ）×ｑ＋１で表される素数Ｎを生成すること
を特徴とする請求項１３記載の鍵発行サーバ。
【請求項１５】
前記素数生成部は、ｌｅｎビットの素数を生成し、
ｌｅｎｑ≧ｌｅｎ／２を満たすｌｅｎｑビットの第１の素数ｑを生成する素数情報生成手段と、
乱数Ｒを生成する乱数生成手段と、
前記発行識別子情報ＩＤＩ、前記第１の素数ｑ、前記乱数Ｒ及び、前記発行識別子情報ＩＤＩと乱数Ｒから整数を生成する単射関数ｆを用いてＮ＝２×ｆ（ＩＤＩ，Ｒ）×ｑ＋１で表される素数候補Ｎを生成する素数候補生成部と、
前記素数候補Ｎに対し、２＾（Ｎ－１）＝１　ｍｏｄ　Ｎを満たすか否かを判定する第１の素数判定部と、
前記素数候補Ｎ及び前記乱数Ｒに対し、２＾（２Ｒ）　≠　１　ｍｏｄ　Ｎを満たすか否かを判定する第２の素数判定部と、を備えること
を特徴とする請求項１３記載の鍵発行サーバ。
【請求項１６】
前記素数生成部は、ｌｅｎビットの素数を生成し、
ｌｅｎｑ≧ｌｅｎ／２を満たすｌｅｎｑビットの第１の素数ｑを生成する素数情報生成手段と、
乱数Ｒを生成する乱数生成手段と、
前記発行識別子情報ＩＤＩ、前記第１の素数ｑ、前記乱数Ｒ及び、前記発行識別子情報ＩＤＩと乱数Ｒから整数を生成する単射関数ｆを用いてＮ＝２×ｆ（ＩＤＩ，Ｒ）×ｑ＋１で表される素数候補Ｎを生成する素数候補生成部と、
前記素数候補Ｎに対し、２＾（Ｎ－１）＝１　ｍｏｄ　Ｎを満たすか否かを判定する第１の素数判定部と、
前記素数候補Ｎ及び前記乱数Ｒに対し、ＧＣＤ（２＾（２Ｒ）－１，Ｎ）＝１を満たすか否かを判定する第２の素数判定部と、を備えること
を特徴とする請求項１３記載の鍵発行サーバ。
【請求項１７】
前記発行識別子情報は、鍵発行サーバを識別する鍵発行サーバ識別子を含むこと
を特徴とする請求項１３から請求項１６のいずれか１項に記載の鍵発行サーバ。
【請求項１８】
前記単射関数ｆは、前記発行識別子情報ＩＤＩと前記乱数Ｒを用いて、ｆ（ＩＤＩ，Ｒ）＝ＩＤＩ｜｜Ｒであること
を特徴とする請求項１３から１７記載の鍵発行サーバ。

【請求項１９】
素数を生成する素数生成装置であって、
前記素数生成装置は、発行識別子を生成する発行識別子生成部と、前記発行識別子情報ＩＤＩに基づいて素数を生成する素数生成部と、を備えること
を特徴とする素数生成装置。
【請求項２０】
前記素数生成部は、第１素数ｑ、乱数Ｒ、前記発行識別子情報ＩＤＩ及び、前記発行識別子情報ＩＤＩと乱数Ｒから整数を生成する単射関数ｆを用いてＮ＝２×ｆ（ＩＤＩ，Ｒ）×ｑ＋１で表される素数Ｎを生成すること
を特徴とする請求項１９記載の素数生成装置。
【請求項２１】
前記素数生成部は、ｌｅｎビットの素数を生成し、
ｌｅｎｑ≧ｌｅｎ／２を満たすｌｅｎｑビットの第１の素数ｑを生成する素数情報生成手段と、
乱数Ｒを生成する乱数生成手段と、
前記発行識別子情報ＩＤＩ、前記第１の素数ｑ、前記乱数Ｒ及び、前記発行識別子情報ＩＤＩと乱数Ｒから整数を生成する単射関数ｆを用いてＮ＝２×ｆ（ＩＤＩ，Ｒ）×ｑ＋１で表される素数候補Ｎを生成する素数候補生成部と、
前記素数候補Ｎに対し、２＾（Ｎ－１）＝１　ｍｏｄ　Ｎを満たすか否かを判定する第１の素数判定部と、
前記素数候補Ｎ及び前記乱数Ｒに対し、２＾（２Ｒ）　≠　１　ｍｏｄ　Ｎを満たすか否かを判定する第２の素数判定部と、を備えること
を特徴とする請求項１９記載の素数生成装置。
【請求項２２】
前記素数生成部は、ｌｅｎビットの素数を生成し、
ｌｅｎｑ≧ｌｅｎ／２を満たすｌｅｎｑビットの第１の素数ｑを生成する素数情報生成手段と、
乱数Ｒを生成する乱数生成手段と、
前記発行識別子情報ＩＤＩ、前記第１の素数ｑ、前記乱数Ｒ及び、前記発行識別子情報ＩＤＩと乱数Ｒから整数を生成する単射関数ｆを用いてＮ＝２×ｆ（ＩＤＩ，Ｒ）×ｑ＋１で表される素数候補Ｎを生成する素数候補生成部と、
前記素数候補Ｎに対し、２＾（Ｎ－１）＝１　ｍｏｄ　Ｎを満たすか否かを判定する第１の素数判定部と、
前記素数候補Ｎ及び前記乱数Ｒに対し、ＧＣＤ（２＾（２Ｒ）－１，Ｎ）＝１を満たすか否かを判定する第２の素数判定部と、を備えること
を特徴とする請求項１９記載の素数生成装置。
【請求項２３】
前記単射関数ｆは、前記発行識別子情報ＩＤＩと前記乱数Ｒを用いて、ｆ（ＩＤＩ，Ｒ）＝ＩＤＩ｜｜Ｒであること
を特徴とする請求項１９から請求項２２のいずれか１項に記載の素数生成装置。
【請求項２４】
鍵発行サーバと、端末装置を備え、前記鍵発行サーバからＲＳＡ暗号の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行方法であって、
前記鍵発行サーバは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成部と、を備え、
前記端末装置は、データを送信する送信部と、データを受信する受信部と、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵を格納する公開鍵格納部と、を備え、
前記素数生成部は、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて前記素数を生成すること

を特徴とする鍵発行方法。

【請求項２５】

鍵発行サーバと、証明書発行サーバと、端末装置を備え、前記鍵発行サーバが素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を生成し、前記証明書発行サーバが前記公開鍵に対する公開鍵証明書を生成し、前記鍵発行サーバが前記秘密鍵及び公開鍵証明書を前記端末装置へ送信する鍵発行方法であって、

前記鍵発行サーバは、データを送信する送信部と、データを受信する受信部と、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成部と、を備え、

前記証明書発行サーバは、前記公開鍵に対する前記公開鍵証明書を生成する公開鍵証明書生成部を備え、

前記端末装置は、データを送信する送信部と、データを受信する受信部と、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵証明書を格納する公開鍵証明書格納部と、を備え、

前記素数生成部は、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて前記素数を生成すること

を特徴とする鍵発行方法。

【請求項２６】

鍵発行サーバと、端末装置を備え、前記鍵発行サーバから素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行システムにおける端末装置に実行させるプログラムであって、

前記プログラムは、素数を含む前記秘密鍵を格納する秘密鍵格納ステップと、前記公開鍵を格納する公開鍵格納ステップと、を前記端末装置に実行させ、

前記秘密鍵は発行識別子情報に基づいて生成された素数を含み、

前記素数は、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて生成されていること

を特徴とするプログラム。

【請求項２７】

鍵発行サーバと、証明書発行サーバと、端末装置を備え、前記鍵発行サーバが素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を生成し、前記証明書発行サーバが前記公開鍵に対する公開鍵証明書を生成し、前記鍵発行サーバが前記秘密鍵及び公開鍵証明書を前記端末装置へ送信する鍵発行システムにおける端末装置に実行させるプログラムであって、

前記プログラムは、前記秘密鍵を格納する秘密鍵格納ステップと、前記公開鍵証明書を格納する公開鍵証明書格納ステップと、を前記端末装置に実行させ、

前記秘密鍵は発行識別子情報に基づいて生成された素数を含み、

前記素数は、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて生成されていること

を特徴とするプログラム。

【請求項２８】

鍵発行サーバと、端末装置を備え、前記鍵発行サーバから素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行システムにおける鍵発行サーバに実行させるプログラムであって、

前記プログラムは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて素数を生成する素数生成ステップと、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成ステップと、を前記鍵発行サーバに実行させ、

前記素数生成ステップは、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて前記素数を生成すること

を特徴とするプログラム。

【請求項２９】

素数を生成する素数生成装置に実行させるプログラムであって、
前記プログラムは、発行識別子を生成する発行識別子生成ステップと、前記発行識別子情報に基づいて素数を生成する素数生成ステップと、を前記素数生成装置に実行させ、
前記素数生成ステップは、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて前記素数を生成すること
を特徴とするプログラム。
【請求項３０】
請求項２６から請求項２９のいずれか１項に記載のプログラムを記録した媒体。

【書類名】明細書
【発明の名称】鍵発行システム、鍵発行装置、素数生成装置、鍵発行方法、素数生成方法及び記録媒体
【技術分野】
【０００１】
本発明は、素因数分解を安全性の根拠として実現する暗号などの情報セキュリティ技術に関する。
【背景技術】
【０００２】
近年、コンピュータ技術及び通信技術に基づくデータ通信が広く普及してきており、このデータ通信においては、秘密通信方式やデジタル署名方式が用いられる。ここで、秘密通信方式とは、特定の通信相手以外に通信内容を漏らすことなく通信を行う方式である。またデジタル署名方式とは、通信相手に通信内容の正当性を示したり、発信者の身元を証明したりする通信方式である。
【０００３】
１．公開鍵暗号方式
これらの秘密通信方式又はデジタル署名方式においては、公開鍵暗号方式とよばれる暗号方式が用いられる。公開鍵暗号方式を用いる秘密通信では、暗号化鍵と復号化鍵とが異なり、復号化鍵は秘密にするが、暗号化鍵は公開する。秘密にする復号化鍵を秘密鍵と呼び、公開する暗号化鍵を公開鍵と呼ぶ。通信相手が多数のとき、共通鍵暗号では通信相手間で鍵をもつ必要があるが、公開鍵暗号では通信相手が一つの固有の鍵をもつだけで通信可能になるため、通信相手が増えても、共通鍵暗号より鍵の数が少なくてよい。このように、公開鍵暗号は多数の通信相手と通信を行うのに適しており、不可欠な基盤技術である。
【０００４】
公開鍵暗号方式の１種であるＲＳＡ暗号方式では、整数の素因数分解問題を解くことが、計算量の上で困難であることを安全性の根拠としている。素因数分解問題とは、ｐ，ｑを素数とし、整数ｎ＝ｐ×ｑとするとき、整数ｎに対して、素数ｐ，ｑを求める問題である。ここで、×は通常の乗算である。一般にｐ，ｑが１０２４ビットの数のように大きい場合は、素因数分解問題が困難である。それにより、ＲＳＡ暗号方式の公開鍵から秘密鍵を求めることや、秘密鍵を持たないユーザが暗号文から平文を求めることが、困難になる。なお、素因数分解問題については、非特許文献１の１４４～１５１ページに詳しく述べられている。
【０００５】
（素因数分解問題を応用するＲＳＡ暗号方式）
ここで、素因数分解問題を応用するＲＳＡ暗号方式について説明する。
（１）鍵の生成
次に示すようにして公開鍵及び秘密鍵を計算する。
・ランダムに大きい素数ｐ，ｑを選択し、その積ｎ＝ｐ×ｑを計算する。
【０００６】
・（ｐ－１）及び（ｑ－１）の最小公倍数Ｌ＝ＬＣＭ（ｐ－１，ｑ－１）を計算する。
・Ｌと互いに素でＬより小さい自然数ｅをランダムに選ぶ。
　　１≦ｅ≦Ｌ－１、ＧＣＤ（ｅ，Ｌ）＝１
ここで、ＧＣＤ（ｅ，Ｌ）は、ｅとＬの最大公約数を示している。
・ｅ×ｄ＝１　ｍｏｄ　Ｌを満たすｄを計算する。ＧＣＤ（ｅ，Ｌ）＝１より、このようなｄは必ず存在する。このようにして、得られた整数ｅ及び整数ｎが、公開鍵である。また、整数ｄが、秘密鍵である。ここで、ｘ　ｍｏｄ　ｙは、ｘをｙで割った余りを示す。
【０００７】
（２）暗号文の生成

公開鍵である整数ｅ及び整数ｎを用いて、平文ｍに暗号演算を施して暗号文ｃを計算する。

ｃ＝ｍ＾ｅ　　ｍｏｄ　　ｎ

なお、この明細書において、演算子＾は、べき乗を示す。例えば、Ａ＾ｘは、　ｘ＞０のときはＡをｘ回乗じたものを示す。

【０００８】

（３）復号文の生成

秘密鍵である整数ｄを用いて、暗号文ｃに復号演算を施して復号文ｍ’を計算する。

ｍ’＝ｃ＾ｄ　　ｍｏｄ　　ｎ

なお、

ｍ’＝ｃ＾ｄ　　ｍｏｄ　　ｎ
＝（ｍ＾ｅ）＾ｄ　　ｍｏｄ　　ｎ
＝ｍ＾（ｅ×ｄ　　ｍｏｄ　　Ｌ）　　ｍｏｄ　　ｎ
＝ｍ＾１　　ｍｏｄ　　ｎ
＝ｍ　　ｍｏｄ　　ｎ

であるので、復号文ｍ’は、平文ｍと一致する。

【０００９】

また、ＲＳＡ暗号については、非特許文献２の１１０～１１３ページに詳しく説明されている。

上記に示した素因数分解を応用したＲＳＡ暗号における公開鍵の生成のステップにおいて、素数生成が行われる。素数生成については、非特許文献３の１４５～１５４ページに詳しく説明されている。素数生成方法には、確率的素数生成法と確定的素数生成方法がある。確率的素数生成法により生成される素数は、「素数である確率が高い」数であり、１００％素数であるとは限らない。一方、確定的素数生成方法は、確実に素数である数を生成する。確率的素数生成方法及び確定的素数生成方法については、非特許文献２に詳しく説明されている。以下では、確定的素数生成方法について説明する。

【００１０】

２．従来例１－確定的素数生成方法

確定的に素数を生成することができるＭａｕｒｅｒ法による確定的素数生成方法について説明する。ここで、Ｍａｕｒｅｒ法については、非特許文献３の１５２～１５３ページに詳しく説明されている。

前記確定的素数生成方法では、次に示すステップを繰り返すことにより、素数を生成する。あらかじめビットサイズｌｅｎｑの素数ｑが与えられている。

【００１１】

（ステップ１）（ｌｅｎｑ－１）ビットの乱数Ｒを選択する。なお、乱数Ｒの先頭ビットは、必ず１となるようにする。

（ステップ２）数Ｎを以下の式により計算する。

Ｎ＝２×ｑ×Ｒ＋１

（ステップ３）数Ｎが素数であるか否かを、次に示す第１判定及び第２判定がともに、成立する場合に、素数と判定する。他の場合に、素数でないと判定する。

【００１２】

（第１判定）　２＾（Ｎ－１）　＝１　　ｍｏｄ　　Ｎ
（第２判定）　ＧＣＤ（２＾（２Ｒ）－１、Ｎ）＝１

素数であると判定される場合には、数Ｎを素数として出力する。素数でないと判定される場合には、ステップ１へ戻って、素数が出力されるまで、処理を繰り返す。

ステップ３で述べられている判定方法は、Ｐｏｃｋｌｉｎｇｔｏｎの素数判定法とよばれ、非特許文献３の１４４ページに詳しく述べられている。Ｐｏｃｋｌｉｎｇｔｏｎ　の素数判定法では、Ｎ＝２×ｑ×Ｒ＋１のｑが素数であり、第１判定及び第２判定の結果が真であれば、必ず、Ｎが素数になる。そのため、確定的に素数であることを判定でき、確定的な素数生成が可能になる。

【００１３】
このようにして、Ｍａｕｒｅｒ法による確定的素数生成方法では、サイズｌｅｎｑの素数ｑを基にして、サイズ２×ｌｅｎｑの素数Ｎを生成する。従って、Ｍａｕｒｅｒ法による確定的素数生成方法を用いて所定長の素数を生成する場合には、前記所定長以下の素数の生成を繰り返し行う。例えば、５１２ビット長の素数を生成する場合には、あらかじめ与えられた８ビットの素数を基にして１６ビットの素数を生成する。次に、生成した１６ビットの素数を基にして３２ビットの素数を生成する。次に、生成した３２ビットの素数を基にして６４ビットの素数を生成する。以下同様の素数生成を繰り返して、５１２ビットの素数を生成する。

【００１４】
なお、前記第２判定を次の判定に代えてもよい。

（第３判定）　　２＾（２Ｒ）≠１　　ｍｏｄ　　Ｎ

上記第３判定方法は、非特許文献４に詳しく述べられている。以降、こちらの判定方法を使用していく。

３．複数の鍵発行サーバをもつ鍵発行システム

公開鍵暗号の鍵発行システムでは、ユーザが鍵を生成する場合や、鍵発行サーバによりユーザに鍵を発行する場合がある。鍵発行サーバにより鍵を発行する場合、ユーザに鍵を発行するサーバは一台であることが多い。しかし、ユーザが増加すると、上記のような素数生成方法は、複数回べき乗を行うことにより計算量が大きいため、計算時間が大きくなってくる。そこで、鍵発行サーバを複数もち、それぞれで鍵発行をすることにより、計算量の分散を図ることがある。そのとき、各ユーザで同じ素数が鍵となった場合、素因数分解ができるため、安全性が著しく低下する。たとえば、ユーザＡの素数をｐＡ１、ｐＡ２とし、ｎＡ＝ｐＡ１×ｐＡ２、ユーザＢの素数をｐＢ１、ｐＢ２とし、ｎＢ＝ｐＢ１×ｐＢ２とする。このとき、ｐＡ１＝ｐＢ１であれば、ユーザＡはＧＣＤ（ｐＡ１，ｎＢ）を求めることにより、ユーザＢの素数の一つがｐＡ１と等しいことがわかり、その結果、ｎＢ／ｐＡ１を計算することにより、ｐＢ２も得ることができる。ＲＳＡ暗号は、素因数分解を安全性の根拠としているため、素因数が判明すると、簡単に解読可能になる。そのため、ユーザＡはユーザＢの公開鍵で暗号化した暗号文を解ける。また、同様に、ユーザＢはユーザＡの公開鍵で暗号化した暗号文を解けてしまう。

【特許文献１】特開２００３－５６４４号公報
【非特許文献１】岡本龍明、太田和夫共編、「暗号・ゼロ知識問題・数論」、共立出版、１９９０
【非特許文献２】岡本龍明、山本博資、”現代暗号”、産業図書（１９９７年）
【非特許文献３】Ａ．Ｊ．　Ｍｅｎｅｚｅｓ，　Ｐ．Ｃ．　ｖａｎ　Ｏｏｒｓｃｈｏｔ，　Ｓ．Ａ．　Ｖａｎｓｔｏｎｅ，　“Ｈａｎｄｂｏｏｋ　ｏｆ　ａｐｐｌｉｅｄ　ｃｒｙｐｔｏｇｒａｐｈｙ”，ＣＲＣ　Ｐｒｅｓｓ，　１９９７
【非特許文献４】岡本　栄司、「暗号理論入門」、共立出版、１９９３、２１ページ

【発明の開示】
【発明が解決しようとする課題】

【００１５】
従来技術では、複数回素数生成を行ったときに素数が一致する可能性があり、それにより、暗号の安全性を著しく低下させるという課題がある。それに対しては、発行済の素数（秘密鍵）と発行した素数を比較することにより、一致しないことを確認できる。しかし、通常の公開鍵暗号のシステムでは、発行した後の公開鍵は鍵発行サーバで管理するが、秘密鍵は機密性が高いため、削除してしまうことが多い。そのため、新たに発行済の素数（秘密鍵）を管理する必要がある。さらに、発行数が１０億個程度に大きさになると、比較する時間が大きく現実的でないという課題がある。

【００１６】
また、複数の鍵発行サーバで発行した場合、すべての鍵発行サーバで発行した素数が一致させないため、各鍵発行サーバ間で、発行した素数、すなわち、秘密鍵を互いにチェッ

クさせる必要がある。各鍵発行サーバ間で信頼関係がある場合は問題ないが、各鍵発行サーバはそれぞれ別の会社が設置することが多いため、信頼できるとは限らない。さらに、もし、各鍵発行サーバ間で信頼関係がある場合であっても、鍵を発行するたびに、各鍵発行サーバの秘密鍵のデータベースにアクセスするため、各鍵発行サーバ間の通信量が大きくなる。このように各鍵発行サーバ間で互いにチェックすることは現実的でないという課題がある。

【００１７】

本発明は、複数回素数生成を行っても、素数が一致しないことを比較することなく、証明できる素数生成方法を提供することを目的とする。

【課題を解決するための手段】

【００１８】

上記目的を達成するために、請求項１における発明は、鍵発行サーバと、端末装置を備え、前記鍵発行サーバから素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行システムであって、前記鍵発行サーバは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成部と、を備え、前記端末装置は、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵を格納する公開鍵格納部と、を備え、前記素数生成部は、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて前記素数を生成することを特徴とする。

【００１９】

請求項２における発明は、鍵発行サーバと、証明書発行サーバと、端末装置を備え、前記鍵発行サーバが素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を生成し、前記証明書発行サーバが前記公開鍵に対する公開鍵証明書を生成し、前記鍵発行サーバが前記秘密鍵及び公開鍵証明書を前記端末装置へ送信する鍵発行システムであって、前記鍵発行サーバは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成部と、を備え、前記証明書発行サーバは、前記公開鍵に対する前記公開鍵証明書を生成する公開鍵証明書生成部を備え、前記端末装置は、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵証明書を格納する公開鍵証明書格納部と、を備え、前記素数生成部は、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて前記素数を生成することを特徴とする。

【００２０】

請求項３における発明は、前記証明書発行サーバは、さらに、前記公開鍵が前記発行識別子に基づいた前記素数を用いて生成されているかを判定する鍵判定部を備えることを特徴とする。

請求項４における発明は、前記素数生成部は、第１素数ｑ、乱数Ｒ、前記発行識別子情報ＩＤＩ及び、前記発行識別子情報ＩＤＩと乱数Ｒから整数を生成する単射関数ｆを用いてＮ＝２×ｆ（ＩＤＩ，Ｒ）×ｑ＋１で表される素数Ｎを生成することを特徴とする。

【００２１】

請求項５における発明は、前記素数生成部は、ｌｅｎビットの素数を生成し、ｌｅｎｑ≧ｌｅｎ／２を満たすｌｅｎｑビットの第１の素数ｑを生成する素数情報生成手段と、乱数Ｒを生成する乱数生成手段と、前記発行識別子情報ＩＤＩ、前記第１の素数ｑ、前記乱数Ｒ及び、前記発行識別子情報ＩＤＩと乱数Ｒから整数を生成する単射関数ｆを用いてＮ＝２×ｆ（ＩＤＩ，Ｒ）×ｑ＋１で表される素数候補Ｎを生成する素数候補生成部と、前記素数候補Ｎに対し、２＾（Ｎ－１）＝１　ｍｏｄ　Ｎを満たすか否かを判定する第１の素数判定部と、前記素数候補Ｎ及び前記乱数Ｒに対し、２＾（２Ｒ）　≠　１　ｍｏｄ　Ｎを満たすか否かを判定する第２の素数判定部と、を備えることを特徴とする（ここで、ａ＾ｘはａのｘ乗を示す）。

【００２２】

請求項６における発明は、前記素数生成部は、ｌｅｎビットの素数を生成し、ｌｅｎｑ

≧ｌｅｎ／２を満たすｌｅｎｑビットの第１の素数ｑを生成する素数情報生成手段と、乱数Ｒを生成する乱数生成手段と、前記発行識別子情報ＩＤＩ、前記第１の素数ｑ、前記乱数Ｒ及び、前記発行識別子情報ＩＤＩと乱数Ｒから整数を生成する単射関数ｆを用いてＮ＝２×ｆ（ＩＤＩ，Ｒ）×ｑ＋１で表される素数候補Ｎを生成する素数候補生成部と、前記素数候補Ｎに対し、２＾（Ｎ－１）＝１　ｍｏｄ　Ｎを満たすか否かを判定する第１の素数判定部と、前記素数候補Ｎ及び前記乱数Ｒに対し、ＧＣＤ（２＾（２Ｒ）－１，Ｎ）＝１を満たすか否かを判定する第２の素数判定部と、を備えることを特徴とする。

【００２３】

請求項７における発明は、前記発行識別子情報は、鍵発行サーバを識別する鍵発行サーバ識別子を含むことを特徴とする。

請求項８における発明は、前記単射関数ｆは、前記発行識別子情報ＩＤＩと前記乱数Ｒを用いて、ｆ（ＩＤＩ，Ｒ）＝ＩＤＩ｜｜Ｒであることを特徴とする（ここで、ａ||ｘはａとｘの連結を示す）。

【００２４】

請求項９における発明は、鍵発行サーバと、端末装置を備え、前記鍵発行サーバから素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行システムにおける端末装置であって、前記端末装置は、素数を含む前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵を格納する公開鍵格納部と、を備え、前記秘密鍵は発行識別子情報に基づいて生成された素数を含み、前記素数は、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて生成されていることを特徴とする。

【００２５】

請求項１０における発明は、鍵発行サーバと、証明書発行サーバと、端末装置を備え、前記鍵発行サーバが素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を生成し、前記証明書発行サーバが前記公開鍵に対する公開鍵証明書を生成し、前記鍵発行サーバが前記秘密鍵及び公開鍵証明書を前記端末装置へ送信する鍵発行システムにおける端末装置であって、前記端末装置は、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵証明書を格納する公開鍵証明書格納部と、を備え、前記秘密鍵は発行識別子情報ＩＤＩに基づいて生成された素数を含み、前記素数は、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて生成されていることを特徴とする。

【００２６】

請求項１１における発明は、前記素数は、第１素数ｑ、乱数Ｒ、前記発行識別子情報ＩＤＩ及び、前記発行識別子情報ＩＤＩと乱数Ｒから整数を生成する単射関数ｆを用いてＮ＝２×ｆ（ＩＤＩ，Ｒ）×ｑ＋１で表されることを特徴とする。

請求項１２における発明は、前記単射関数ｆは、前記発行識別子情報ＩＤＩと前記乱数Ｒを用いて、ｆ（ＩＤＩ，Ｒ）＝ＩＤＩ｜｜Ｒであることを特徴とする。

【００２７】

請求項１３における発明は、鍵発行サーバと、端末装置を備え、前記鍵発行サーバから素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行システムにおける鍵発行サーバであって、前記鍵発行サーバは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成部と、を備え、前記素数生成部は、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて前記素数を生成することを特徴とする。

【００２８】

請求項１４における発明は、前記素数生成部は、第１素数ｑ、乱数Ｒ、前記発行識別子情報ＩＤＩ及び、前記発行識別子情報ＩＤＩと乱数Ｒから整数を生成する単射関数ｆを用いてＮ＝２×ｆ（ＩＤＩ，Ｒ）×ｑ＋１で表される素数Ｎを生成することを特徴とする。

請求項１５における発明は、前記素数生成部は、ｌｅｎビットの素数を生成し、ｌｅｎｑ≧ｌｅｎ／２を満たすｌｅｎｑビットの第１の素数ｑを生成する素数情報生成手段と、乱数Ｒを生成する乱数生成手段と、前記発行識別子情報ＩＤＩ、前記第１の素数ｑ、前記

乱数Ｒ及び、前記発行識別子情報ＩＤＩと乱数Ｒから整数を生成する単射関数ｆを用いてＮ＝２×ｆ（ＩＤＩ，Ｒ）×ｑ＋１で表される素数候補Ｎを生成する素数候補生成部と、前記素数候補Ｎに対し、２＾（Ｎ－１）＝１　ｍｏｄ　Ｎを満たすか否かを判定する第１の素数判定部と、前記素数候補Ｎ及び前記乱数Ｒに対し、２＾（２Ｒ）　≠　１　ｍｏｄ　Ｎを満たすか否かを判定する第２の素数判定部と、を備えることを特徴とする。

【００２９】

請求項１６における発明は、前記素数生成部は、ｌｅｎビットの素数を生成し、ｌｅｎｑ≧ｌｅｎ／２を満たすｌｅｎｑビットの第１の素数ｑを生成する素数情報生成手段と、乱数Ｒを生成する乱数生成手段と、前記発行識別子情報ＩＤＩ、前記第１の素数ｑ、前記乱数Ｒ及び、前記発行識別子情報ＩＤＩと乱数Ｒから整数を生成する単射関数ｆを用いてＮ＝２×ｆ（ＩＤＩ，Ｒ）×ｑ＋１で表される素数候補Ｎを生成する素数候補生成部と、前記素数候補Ｎに対し、２＾（Ｎ－１）＝１　ｍｏｄ　Ｎを満たすか否かを判定する第１の素数判定部と、前記素数候補Ｎ及び前記乱数Ｒに対し、ＧＣＤ（２＾（２Ｒ）－１，Ｎ）＝１を満たすか否かを判定する第２の素数判定部と、を備えることを特徴とする。

【００３０】

請求項１７における発明は、前記発行識別子情報は、鍵発行サーバを識別する鍵発行サーバ識別子を含むことを特徴とする。

請求項１８における発明は、前記単射関数ｆは、前記発行識別子情報ＩＤＩと前記乱数Ｒを用いて、ｆ（ＩＤＩ，Ｒ）＝ＩＤＩ｜｜Ｒであることを特徴とする。

請求項１９における発明は、素数を生成する素数生成装置であって、前記素数生成装置は、発行識別子を生成する発行識別子生成部と、前記発行識別子情報ＩＤＩに基づいて素数を生成する素数生成部と、を備えることを特徴とする。

【００３１】

請求項２０における発明は、前記素数生成部は、第１素数ｑ、乱数Ｒ、前記発行識別子情報ＩＤＩ及び、前記発行識別子情報ＩＤＩと乱数Ｒから整数を生成する単射関数ｆを用いてＮ＝２×ｆ（ＩＤＩ，Ｒ）×ｑ＋１で表される素数Ｎを生成することを特徴とする。

請求項２１における発明は、前記素数生成部は、ｌｅｎビットの素数を生成し、ｌｅｎｑ≧ｌｅｎ／２を満たすｌｅｎｑビットの第１の素数ｑを生成する素数情報生成手段と、乱数Ｒを生成する乱数生成手段と、前記発行識別子情報ＩＤＩ、前記第１の素数ｑ、前記乱数Ｒ及び、前記発行識別子情報ＩＤＩと乱数Ｒから整数を生成する単射関数ｆを用いてＮ＝２×ｆ（ＩＤＩ，Ｒ）×ｑ＋１で表される素数候補Ｎを生成する素数候補生成部と、前記素数候補Ｎに対し、２＾（Ｎ－１）＝１　ｍｏｄ　Ｎを満たすか否かを判定する第１の素数判定部と、前記素数候補Ｎ及び前記乱数Ｒに対し、２＾（２Ｒ）　≠　１　ｍｏｄ　Ｎを満たすか否かを判定する第２の素数判定部と、を備えることを特徴とする。

【００３２】

請求項２２における発明は、前記素数生成部は、ｌｅｎビットの素数を生成し、ｌｅｎｑ≧ｌｅｎ／２を満たすｌｅｎｑビットの第１の素数ｑを生成する素数情報生成手段と、乱数Ｒを生成する乱数生成手段と、前記発行識別子情報ＩＤＩ、前記第１の素数ｑ、前記乱数Ｒ及び、前記発行識別子情報ＩＤＩと乱数Ｒから整数を生成する単射関数ｆを用いてＮ＝２×ｆ（ＩＤＩ，Ｒ）×ｑ＋１で表される素数候補Ｎを生成する素数候補生成部と、前記素数候補Ｎに対し、２＾（Ｎ－１）＝１　ｍｏｄ　Ｎを満たすか否かを判定する第１の素数判定部と、前記素数候補Ｎ及び前記乱数Ｒに対し、ＧＣＤ（２＾（２Ｒ）－１，Ｎ）＝１を満たすか否かを判定する第２の素数判定部と、を備えることを特徴とする。

【００３３】

請求項２３における発明は、前記単射関数ｆは、前記発行識別子情報ＩＤＩと前記乱数Ｒを用いて、ｆ（ＩＤＩ，Ｒ）＝ＩＤＩ｜｜Ｒであることを特徴とする。

請求項２４における発明は、鍵発行サーバと、端末装置を備え、前記鍵発行サーバからＲＳＡ暗号の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行方法であって、前記鍵発行サーバは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵

生成部と、を備え、前記端末装置は、データを送信する送信部と、データを受信する受信部と、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵を格納する公開鍵格納部と、を備え、前記素数生成部は、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて前記素数を生成することを特徴とする。

【００３４】

請求項２５における発明は、鍵発行サーバと、証明書発行サーバと、端末装置を備え、前記鍵発行サーバが素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を生成し、前記証明書発行サーバが前記公開鍵に対する公開鍵証明書を生成し、前記鍵発行サーバが前記秘密鍵及び公開鍵証明書を前記端末装置へ送信する鍵発行方法であって、前記鍵発行サーバは、データを送信する送信部と、データを受信する受信部と、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成部と、を備え、前記証明書発行サーバは、前記公開鍵に対する前記公開鍵証明書を生成する公開鍵証明書生成部を備え、前記端末装置は、データを送信する送信部と、データを受信する受信部と、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵証明書を格納する公開鍵証明書格納部と、を備え、前記素数生成部は、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて前記素数を生成することを特徴とする。

【００３５】

請求項２６における発明は、鍵発行サーバと、端末装置を備え、前記鍵発行サーバから素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行システムにおける端末装置に実行させるプログラムであって、前記プログラムは、素数を含む前記秘密鍵を格納する秘密鍵格納ステップと、前記公開鍵を格納する公開鍵格納ステップと、を前記端末装置に実行させ、前記秘密鍵は発行識別子情報に基づいて生成された素数を含み、前記素数は、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて生成されていることを特徴とする。

【００３６】

請求項２７における発明は、鍵発行サーバと、証明書発行サーバと、端末装置を備え、前記鍵発行サーバが素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を生成し、前記証明書発行サーバが前記公開鍵に対する公開鍵証明書を生成し、前記鍵発行サーバが前記秘密鍵及び公開鍵証明書を前記端末装置へ送信する鍵発行システムにおける端末装置に実行させるプログラムであって、前記プログラムは、前記秘密鍵を格納する秘密鍵格納ステップと、前記公開鍵証明書を格納する公開鍵証明書格納ステップと、を前記端末装置に実行させ、前記秘密鍵は発行識別子情報に基づいて生成された素数を含み、前記素数は、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて生成されていることを特徴とする。

【００３７】

請求項２８における発明は、鍵発行サーバと、端末装置を備え、前記鍵発行サーバから素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行システムにおける鍵発行サーバに実行させるプログラムであって、前記プログラムは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて素数を生成する素数生成ステップと、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成ステップと、を前記鍵発行サーバに実行させ、前記素数生成ステップは、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて前記素数を生成することを特徴とする。

【００３８】

請求項２９における発明は、素数を生成する素数生成装置に実行させるプログラムであって、前記プログラムは、発行識別子を生成する発行識別子生成ステップと、前記発行識別子情報に基づいて素数を生成する素数生成ステップと、を前記素数生成装置に実行させ、前記素数生成ステップは、前記発行識別子情報と乱数から素数を生成する素数生成単射関数を用いて前記素数を生成することを特徴とする。

【００３９】
請求項３０における発明は、請求項２６から請求項２９のいずれか１項に記載のプログラムを記録した媒体である。
【発明の効果】
【００４０】
これらの構成によると、複数回素数生成を行っても、素数が一致しないことを比較することなく、証明できる素数生成を実現でき、その価値は大きい。
【発明を実施するための最良の形態】
【００４１】
（実施の形態１）
本発明に係る１の実施の形態としての素数生成装置１について説明する。
図１は、実施の形態１における素数生成装置の構成を示す図である。
この素数生成装置１は、素数ｑ、ｑのビットサイズｌｅｎｑ、発行識別子情報ＩＤＩ及び発行識別子情報のビットサイズｌｅｎＩＤＩが与えられたとき、ｑのビットサイズｌｅｎｑの２倍のビットサイズ２×ｌｅｎｑをもつ素数Ｎを出力するものである。
【００４２】
＜素数生成装置１の構成＞
素数生成装置１は、乱数生成部１１と、素数候補生成部１２、第１素数判定部１３と、第２素数判定部１４を備える。
乱数生成部１１は、ｌｅｎｑを用いて、（ｌｅｎｑ－ｌｅｎＩＤＩ－１）ビットの乱数Ｒを生成する。ここで、乱数Ｒ’の最上位ビットは１とする。乱数生成方法は、非特許文献２が詳しい。
【００４３】
素数候補生成部１２は、ｑ及びＲ’を用いて、以下の式を満たすＲとＮを生成する。

$$R = f(IDI \| R')$$
$$N = 2 \times R \times q + 1$$

ここで、ｆは単射である関数であり、例えば、ｆ（ＩＤＩ｜｜Ｒ’）＝Ｅｎｃ（Ｋ，ＩＤＩ｜｜Ｒ’）である。Ｅｎｃ（Ｋ，ＩＤＩ）は鍵Ｋを用いたときのＩＤＩの共通鍵暗号による暗号文である。共通鍵暗号の暗号化関数は一般的に全単射である。また、｜｜はビットまたはバイト連結である。
【００４４】
第１素数判定部１３は、Ｎを用いて、以下の式の成立を判定する。

$$2^{(N-1)} = 1 \mod N \quad (eq1)$$

ここで、２＾（Ｎ－１）は、２のＮ－１乗を示している。
第２素数判定部１４は、ＮとＲを用いて、以下の式の成立を判定する。

$$2^{(2R)} \neq 1 \mod N \quad (eq2)$$

＜素数生成装置１の動作＞
以下に素数生成装置１の動作を示す。図２にこの動作のフローチャートを示す。
【００４５】
ステップＳ１０１：乱数生成部１１は、（ｌｅｎｑ－ｌｅｎＩＤＩ－１）ビットの乱数Ｒ’を生成する。ここで、乱数Ｒ’の最上位ビットは１とする。
ステップＳ１０２：素数候補生成部１２は、以下の式を満たすＲとＮを生成する。

$$R = f(IDI \| R')$$
$$N = 2 \times R \times q + 1$$

ステップＳ１０３：第１素数判定部１３は、$2^{(N-1)} = 1 \mod N$の成立を判定する。この式が成立する場合は次のステップへ。成立しない場合はステップＳ１０１へ。
【００４６】
ステップＳ１０４：第２素数判定部１４は、$2^{(2R)} \neq 1 \mod N$の成立を判定する。この式が成立する場合はＮを出力し、終了する。成立しない場合は、ステッ

プＳ１０１へ。
＜素数生成装置１の動作検証＞
第１素数判定部及び、第２素数判定部は、Ｐｏｃｋｌｉｎｇｔｏｎ判定である。　Ｐｏｃｋｌｉｎｇｔｏｎ判定は、非特許文献１の１４４ページ及び非特許文献４が詳しい。
【００４７】
Ｎ＝２×Ｒ×ｑ＋１のｑが素数であり
２＾（Ｎ－１）　＝　１　ｍｏｄ　Ｎ
２＾（２Ｒ）　≠１　ｍｏｄ　Ｎ
の両方が成り立つ場合、Ｎが素数になるので、素数生成装置１は素数を出力する。
また、乱数Ｒ’のビットサイズが（ｌｅｎｑ－ｌｅｎＩＤ－１）であるので、Ｒのビットサイズが（ｌｅｎｑ－１）になり、ほとんどのＮのビットサイズが２×ｌｅｎｑになる。ここで、ｑやＩＤＩなどの値によっては、ビットサイズが２×ｌｅｎｑ－１となる場合がある。その場合は、素数候補生成部１２で、Ｒ’に２を掛けて、それを新たにＲ’とみなすことにより、Ｎのビットサイズを２×ｌｅｎｑになるように設定する。
【００４８】
＜実施の形態１の効果＞
発行識別子情報ＩＤＩが異なれば、出力される素数Ｎが異なること（＊）を以下で述べる。まず、以下の補題を証明し、その補題を用いて（＊）を証明する。
（補題）二つの素数ｐ１＝２×ｑ１×Ｒ１＋１，　ｐ２　＝２×ｑ２×Ｒ２＋１に対し、ｐ１＝ｐ２であれば、ｑ１＝ｑ２かつＲ１＝Ｒ２　（証明）ｐ１＝ｐ２の場合、ｑ１，ｑ２：２５６ビットの素数であり、Ｒ１，Ｒ２：２５５ビットであるため、ｑ１＝ｑ２となるのは明らか。また、ｑ１＝ｑ２より、Ｒ１＝Ｒ２も成り立つ（証明終）。
【００４９】
上記補題より、ｐ１＝ｐ２であれば、Ｒ１＝Ｒ２が成り立つ。Ｒ１＝ｆ（ＩＤＩ１｜｜Ｒ’１）、Ｒ２＝ｆ（ＩＤＩ２｜｜Ｒ’２）とおくと、Ｒ１＝Ｒ２であり、ｆは単射であるため、ＩＤＩ１＝ＩＤＩ２である。したがって、この対偶を取ることにより、（＊）が成り立つ。　以上より、ＩＤＩが異なれば必ず素数が異なる。したがって、ＩＤＩを毎回変えることで、毎回異なる素数を生成することができる。ＩＤＩはカウンタでもよく、発行のたびにインクリメントしていくことで、容易に毎回異なる素数を生成できることになる。したがって、複数回生成した素数が一致しないことを比較することなく、証明できる。
【００５０】
（実施の形態２）
本発明に係る２の実施の形態としての素数生成装置２について、説明する。
図３は、実施の形態２における素数生成装置の構成を示す図である。
この素数生成装置２は、素数ｑ１、ｑ１のビットサイズｌｅｎｑ１、発行識別子情報ＩＤＩ及び発行識別子情報のビットサイズｌｅｎＩＤＩが与えられたとき、ｑ１のビットサイズｌｅｎｑ１の４倍のビットサイズ４×ｌｅｎｑ１をもつ素数を出力するものである。
【００５１】
＜素数生成装置２の構成＞
素数生成装置２は、実施の形態１と同様の第１素数判定部１３と、第２素数判定部１４と、実施の形態１と異なる素数シード生成部２１と、乱数生成部２２と、素数候補生成部２３と、を備える。
素数シード生成部２１は、素数生成装置１を用いて、ｑ１のビットサイズの２倍のビットサイズをもつ素数ｑ２を生成する。
【００５２】
乱数生成部２２は、ｌｅｎｑ１を用いて、（２×ｌｅｎｑ１－ｌｅｎＩＤＩ－１）ビットの乱数Ｒ’を生成する。ここで、Ｒ’の最上位ビットは１とする。
素数候補生成部２３は、ｑ２及びＲ’を用いて、以下の式を満たすＲとＮを生成する。
Ｒ＝ＩＤＩ×Ｒ’

【００５３】

Ｎ＝２×Ｒ×ｑ２＋１

＜素数生成装置２の動作＞

以下に素数生成装置２の動作を示す。図４にこの動作のフローチャートを示す。

ステップＳ２０１：素数シード生成部２１は、素数ｑ２を生成する。

ステップＳ２０２：乱数生成部２２は、（２×ｌｅｎｑ１－ｌｅｎＩＤＩ－１）ビットの乱数Ｒ’を生成する。ここで、Ｒ’の最上位ビットは１とする。

【００５４】

ステップＳ２０３：素数候補生成部２３は、ＲとＮを計算する。

ステップＳ２０４：第１素数判定部１３は、２＾（Ｎ－１）　＝　１　ｍｏｄ　Ｎの成立を判定する。この式が成立する場合は次のステップＳ２０５へ。成立しない場合はステップＳ２０２へ。

ステップＳ２０５：第２素数判定部１４は、２＾（２Ｒ）　≠　１　ｍｏｄ　Ｎの成立を判定する。この式が成立する場合はＮを出力し、終了する。成立しない場合は、ステップＳ２０２へ。

【００５５】

＜実施の形態２の効果＞

発行識別子情報ＩＤＩが異なれば、出力される素数Ｎが異なることが実施の形態１と同様にいえる。以下に説明する。素数生成装置２で生成した二つの素数Ｎ１＝２×ｑ１１×Ｒ１＋１、Ｎ２＝２×ｑ１２×Ｒ２＋１に対し、二つの素数の発行識別子ＩＤＩが異なれば、ｑ１１≠ｑ１２であるため、先に述べた補題よりＮ１≠Ｎ２である。以上より、ＩＤＩが異なれば必ず素数が異なる。

【００５６】

また、生成された素数Ｎに対して、Ｎ－１は必ず発行識別子情報ＩＤＩで割り切れる。なぜなら、Ｎ－１＝２×ｑ２×ＩＤＩ×Ｒ’が成り立つためである。したがって、生成された素数Ｎに対し、Ｎ－１が発行識別子情報ＩＤＩで割り切れるか否かで、素数生成装置２を用いて素数が生成されたかを確認することができる。

（実施の形態３）

本発明に係る３の実施の形態としての素数生成装置３について、説明する。

【００５７】

図５は、実施の形態３における素数生成装置の構成を示す図である。

この素数生成装置３は、素数ｑ、ｑのビットサイズｌｅｎｑ、発行識別子情報ＩＤＩ及び発行識別子情報のビットサイズｌｅｎＩＤＩが与えられたとき、ｑのビットサイズｌｅｎｑの２倍のビットサイズ２×ｌｅｎｑをもつ素数を出力するものである。

＜素数生成装置３の構成＞

素数生成装置３は、実施の形態１と同様の第１素数判定部１３と、第２素数判定部１４と、実施の形態１と異なる識別子素数生成部３１と、乱数生成部３２と、素数候補生成部３３と、を備える。

【００５８】

識別子素数生成部３１は、予め与えられた素数ｑｇと発行識別子情報ＩＤＩより、素数ｐＩＤＩ＝ｇｐ（ＩＤＩ，ｑｇ）を生成する。ｇｐは発行識別子ＩＤＩと素数ｑｇから一意的に素数を生成する素数生成関数である。例えば、ｇｐ（ＩＤＩ，ｑｇ）は、以下のように求める。ｃ＝０として、２×ｑｇ×ｆ（ＩＤＩ｜｜ｃ）＋１が素数であるかを判定する。素数である場合は、ｇｐ（ＩＤＩ，ｑｇ）＝２×ｑｇ×ｆ（ＩＤＩ｜｜ｃ）＋１とする。素数でなければ、ｃに１加算して２×ｑｇ×ｆ（ＩＤＩ｜｜ｃ）＋１が素数であるかを判定する。素数であれば、ｇｐ（ＩＤＩ，ｑｇ）＝２×ｑｇ×ｆ（ＩＤＩ｜｜ｃ）＋１とする。素数でなければ、ｃに１加算して同様の判定を行い素数になるまで繰り返す。

【００５９】

また、ｌｅｎｑｇはｑｇのビットサイズである。このように関数ｇｐを定義するとき、ｑｇを保持していれば、発行識別子情報ＩＤＩに対して、何回素数生成関数により素数を

生成しても、同じ素数を生成可能である。
乱数生成部３２は、（ｌｅｎｑ－２×ｌｅｎｑｇ－１）ビットの乱数Ｒを生成する。ここで、Ｒの最上位ビットは１とする。
【００６０】
素数候補生成部３３は、素数ｑ，ｐＩＤＩ及び乱数Ｒを用いて、以下の式を満たすＮを生成する。

$$N = 2 \times R \times q \times pIDI + 1$$

＜素数生成装置３の動作＞
以下に素数生成装置３の動作を示す。図６にこの動作のフローチャートを示す。
【００６１】
ステップＳ３０１：識別子素数生成部３１は、素数ｐＩＤＩを生成する。
ステップＳ３０２：乱数生成部３２は、乱数Ｒを生成する。
ステップＳ３０３：素数候補生成部３３は、Ｎ＝２×Ｒ×ｑ×ｐＩＤＩ＋１に設定する。
ステップＳ３０４：第１素数判定部１３は、２＾（Ｎ－１）　＝　１　ｍｏｄ　Ｎの成立を判定する。この式が成立する場合は次のステップＳ３０５へ。成立しない場合は、ステップＳ３０２へ。
【００６２】
ステップＳ３０５：第２素数判定部１４は、２＾（２Ｒ）　≠　１　ｍｏｄ　Ｎの成立を判定する。この式が成立する場合はＮを出力し、終了する。成立しない場合は、ステップＳ３０２へ。
＜実施の形態３の効果＞
発行識別子情報ＩＤＩが異なれば、素数が異なることが実施の形態１、２と同様にいえる。
【００６３】
また、生成された素数Ｎに対して、Ｎ－１は、素数生成関数により生成されるｇｐ（ＩＤＩ，ｑｇ）で割り切れる。したがって、生成された素数が、ｇｐ（ＩＤＩ，ｑｇ）で割り切れるか否かで素数生成装置３を用いて素数が生成されたかを確認することができる。
（実施の形態４）
本発明に係る４の実施の形態としての鍵発行システム４について、説明する。
図７は、実施の形態４における鍵発行システム４の構成を示す図である。本システムは、鍵発行サーバＡ４１、Ｂ４２、Ｃ４３と、証明書発行サーバ４４と、端末装置４５１、４５２、４５３、．．．、４５ｎから構成される。ｎは自然数であり、例えば１０００である。この場合、端末装置が１０００台存在することになる。
【００６４】
＜鍵発行サーバＡ４１、Ｂ４２、Ｃ４３の構成＞
鍵発行サーバＡ４１、Ｂ４２、Ｃ４３は同じ構成であるため、以下では代表して鍵発行サーバＡ４１の構成を示す。鍵発行サーバＡ４１、Ｂ４２、Ｃ４３にはそれぞれ、予め識別子：ＳＩＤＡ、ＳＩＤＢ、ＳＩＤＣが与えられている。
鍵発行サーバＡ４１は、ＲＳＡ暗号における秘密鍵及び公開鍵を生成し、公開鍵を証明書発行サーバへ送信し、公開鍵証明書を受信した後、端末装置へ送信する。
【００６５】
鍵発行サーバＡ４１は、送信部４１０１と、受信部４１０２と、識別子生成部４１０３、識別子格納部４１０４と、素数生成部４１０５と、秘密鍵判定部４１０６と、鍵生成部４１０７と、秘密鍵格納部４１０８と、公開鍵格納部４１０９と、証明書格納部４１１０を備える（図８参照）。
送信部４１０１は、端末装置４５ｉ（ｉ＝１～ｎ）へ生成した秘密鍵及び公開鍵を、証明書発行サーバ４４へ公開鍵を送信する。
【００６６】
受信部４１０２は、端末装置４５ｉから鍵生成要求情報を、証明書発行サーバ４４から

公開鍵証明書Ｃｅｒｔを受信する。公開鍵証明書については、証明書発行サーバ４４の構成の説明で述べる。

識別子生成部４１０３は、端末装置４５ｉ用に素数の発行識別子情報ＩＤＩを生成し、識別子格納部４１０４に格納する。発行識別子情報ＩＤＩは、予め与えられた各鍵発行サーバに対応する識別子：ＳＩＤ（Ａ４１はＳＩＤＡ、Ｂ４２はＳＩＤＢ、Ｃ４３はＳＩＤＣ）と発行識別子：ＰＩＤからなる。例えば、ＩＤＩ＝ＳＩＤ｜｜ＰＩＤとする。ここで、｜｜はビットまたはバイト連結である。発行識別子は例えば、１から発行順に数字を割り当て、発行するたびにインクリメントする。

【００６７】

識別子格納部４１０４は、素数の発行識別子情報ＩＤＩを格納する。

素数生成部４１０５は、５１２ビット素数を生成する。なお、ここでは鍵長が１０２４ビットのＲＳＡを想定しているため、５１２ビット素数を生成するとしたが、鍵長をｌｅｎビットとして、ｌｅｎ／２ビットの素数を生成するとしてもよい。

（素数生成部４１０５の構成及び動作）

素数生成部４１０５は、第１の素数生成部４１０５１と、第２の素数生成部４１０５２と、を備える（図９参照）。

【００６８】

第１の素数生成部４１０５１は、１２８ビットの素数ｑを生成する。素数の生成方法は従来の方法を用いる。従来の方法については、特許文献１及び非特許文献３が詳しい。

第２の素数生成部４１０５２は、１２８ビット素数ｑと、ｑのビットサイズ１２８と、発行識別子情報ＩＤＩを用いて、５１２ビットの素数Ｎを生成する。第２の素数生成部４１０５２は、素数生成装置２を用いて、素数Ｎを生成する。

【００６９】

秘密鍵判定部４１０６は、２回の素数生成部４１０５の処理を実行して出力された素数ｐ１とｐ２が一致しているかを比較する。

鍵生成部４１０７は、秘密鍵格納部４１０８に格納されている秘密鍵ｐ１、ｐ２の積ｎ＝ｐ１×ｐ２を計算し、さらに、乱数ｅを生成し、それらのｎとｅの組ＰＫ＝（ｎ，ｅ）を公開鍵とする。

【００７０】

その後、ｅ×ｄ＝１　ｍｏｄ　Ｌを満たすｄを計算し秘密鍵とする。ここで、Ｌ＝ＬＣＭ（ｐ１－１，ｐ２－１）である。ＬＣＭ（ｐ１－１，ｐ２－１）はｐ１－１とｐ２－１の最小公倍数を示す。

秘密鍵格納部４１０８は、素数生成部４１０５で生成した２つの素数ｐ１、ｐ２と鍵生成部で作成したｄの組ＳＫ＝（ｐ１，ｐ２，ｄ）を秘密鍵として格納する。

【００７１】

公開鍵格納部４１０９は、鍵生成部４１０７で生成した公開鍵ＰＫを格納する。

証明書格納部４１１０は、証明書発行サーバ４４が送信した公開鍵証明書Ｃｅｒｔを格納する。

＜鍵発行サーバＡ４１、Ｂ４２、Ｃ４３の動作＞

鍵発行サーバＡ４１、Ｂ４２、Ｃ４３の動作は同様であるため、以下に代表して鍵発行サーバＡ４１の動作を示す。ここでは、端末装置４５ｉ（ｉは１からｎのいずれかの数）から鍵発行依頼情報が送信された場合の動作を示している。図１０にこの動作のフローチャートを示す。

【００７２】

ステップＳ４０１：受信部４１２は、端末装置４５ｉより送信された鍵発行依頼情報を受信する。

ステップＳ４０２：識別子生成部４１３は、発行識別子情報：ＩＤＩを生成し、識別子格納部４１４に格納する。

ステップＳ４０３：素数生成部４１５は、素数ｐ１を生成する。

【００７３】

ステップＳ４０４：素数生成部４１５は、素数ｐ２を生成する。
ステップＳ４０５：秘密鍵判定部４１６は、素数ｐ１とｐ２がｐ１＝ｐ２を満たすかを判定する。ｐ１＝ｐ２の場合は、ステップＳ４０４へ。それ以外は、秘密鍵格納部４１８に格納する。次のステップＳ４０６へ。
ステップＳ４０６：鍵生成部４１７は、ｎ＝ｐ１×ｐ２を計算する。また、鍵生成部４１７は、乱数ｅを生成し、ｎとｅの組ＰＫ＝（ｎ，ｅ）を公開鍵として公開鍵格納部４１９に格納する。さらに、鍵生成部４１７は、ｅ×ｄ＝１　ｍｏｄ　Ｌを満たすｄを計算し、ｐ１、ｐ２とｄの組ＳＫ＝（ｐ１，ｐ２，ｄ）を秘密鍵として秘密鍵格納部４１８に格納する。

【００７４】

ステップＳ４０７：送信部４１１は、公開鍵格納部４１９に格納されている公開鍵ＰＫ及び識別子格納部４１４に格納されている発行識別子情報ＩＤＩを証明書発行サーバ４４へ送信する。
ステップＳ４０８：受信部４１２は、証明書発行サーバ４４より送信された公開鍵証明書Ｃｅｒｔを受信する。

【００７５】

ステップＳ４０９：送信部４１１は、秘密鍵格納部４１８に格納されている秘密鍵ＳＫ＝（ｐ１，ｐ２，ｄ）と、公開鍵証明書Ｃｅｒｔを端末装置４５ｉへ送信する。終了する。

＜証明書発行サーバ４４の構成＞

証明書発行サーバ４４は、送信部４４１と、受信部４４２と、秘密鍵格納部４４３と、発行公開鍵確認部４４４と、発行公開鍵格納部４４５と、発行識別子情報格納部４４６と、公開鍵証明書生成部４４７と、公開鍵証明書格納部４４８と、を備える（図１１参照）。

【００７６】

送信部４４１は、証明書Ｃｅｒｔを鍵発行サーバＡ４１、Ｂ４２または、Ｃ４３へ送信する。
受信部４４２は、鍵発行サーバＡ４１、Ｂ４２または、Ｃ４３から公開鍵ｎ、ｅを受信する。
秘密鍵格納部４４３は、証明書発行サーバ４４の秘密鍵ＳＫＣＡを格納する。

【００７７】

発行公開鍵確認部４４４は、鍵発行サーバＡ４１、Ｂ４２またはＣ４３から受信した公開鍵ＰＫ＝（ｎ，ｅ）と発行識別子情報ＩＤＩを用いて、公開鍵ＰＫ＝（ｎ，ｅ）が発行識別子情報ＩＤＩを用いて生成されたかを確認する。具体的には、ｎ－１がＩＤＩで割り切れるか否かでチェックする。割り切れる場合は、公開鍵ＰＫ＝（ｎ，ｅ）が発行識別子情報ＩＤＩで生成されたと判断し、それ以外は発行識別子情報ＩＤＩで生成されていないと判断する。

【００７８】

発行公開鍵格納部４４５は、鍵発行サーバＡ４１、Ｂ４２またはＣ４３から受信した公開鍵ＰＫ＝（ｎ，ｅ）を格納する。
発行識別子情報格納部４４６は、鍵発行サーバＡ４１、Ｂ４２またはＣ４３から受信した発行識別子情報ＩＤＩを格納する。
公開鍵証明書生成部４４７は、公開鍵ＰＫと発行識別子情報ＩＤＩに対する公開鍵証明書Ｃｅｒｔを、秘密鍵格納部４４３に格納されている秘密鍵ＳＫＣＡを用いて生成する。具体的には、例えば、Ｃｅｒｔ＝ｎ｜｜ｅ｜｜ＩＤＩ｜｜Ｓｉｇ（ＳＫＣＡ，ｎ｜｜ｅ｜｜ＩＤＩ）とする。ここで、Ｓｉｇ（Ｋ，Ｄ）はデータＤに対する鍵Ｋを用いたときの署名データである。また、｜｜はビットまたはバイトの連結である。

【００７９】

公開鍵証明書格納部４４８は、公開鍵証明書Ｃｅｒｔを格納する。

＜証明書発行サーバ４４の動作＞

以下に証明書発行サーバ４４の動作を示す。ここでは、証明書を発行する先を鍵発行サーバＡ４１として動作を示す。なお、他の鍵発行サーバ（Ｂ４２、Ｃ４３）を発行先の場合も同様の動作を行う。図１２にこの動作のフローチャートを示す。

【００８０】

ステップＳ５０１：受信部４４２は、鍵発行サーバＡ４１から送信された公開鍵ＰＫ＝（ｎ，ｅ）と発行識別子情報ＩＤＩを受信する。

ステップＳ５０２：発行公開鍵確認部４４４は、公開鍵ＰＫ＝（ｎ，ｅ）が発行識別子情報ＩＤＩを用いて生成されたかを確認する。公開鍵ＰＫ＝（ｎ，ｅ）が発行識別子情報ＩＤＩで生成されていると判断した場合は、次のステップＳ５０３へ。それ以外は、システムを終了する。

【００８１】

ステップＳ５０３：発行公開鍵格納部４４５は、公開鍵ＰＫ＝（ｎ，ｅ）を、発行識別子情報格納部４４６は、発行識別子情報ＩＤＩをそれぞれ格納する。

ステップＳ５０４：公開鍵証明書生成部４４７は、公開鍵ＰＫ＝（ｎ，ｅ）と発行識別子情報ＩＤＩに対する公開鍵証明書Ｃｅｒｔを生成し、公開鍵証明書格納部４４８に格納する。

【００８２】

ステップＳ５０５：送信部４４１は、公開鍵証明書格納部４４８に格納されている公開鍵証明書Ｃｅｒｔを鍵発行Ａ４１へ送信し、終了する。

＜端末装置４５ｉ（ｉ＝１～ｎ）の構成＞

端末装置４５１、４５２、４５３、．．．、４５ｎはそれぞれ、同じ構成をしているため、以下では代表して、端末装置４５ｉの構成を示す。

【００８３】

端末装置４５ｉは、送信部４５ｉ１と、受信部４５ｉ２と、秘密鍵格納部４５ｉ３と、公開鍵格納部４５ｉ４と、発行識別子情報格納部４５ｉ５と、を備える（図１３参照）。

送信部４５ｉ１は、鍵発行依頼情報を鍵発行サーバＡ４１、Ｂ４２、Ｃ４３のいずれかへ送信する。鍵発行依頼情報は、例えば、端末装置４５ｉを示す識別子情報などである。

受信部４５ｉ２は、鍵発行サーバＡ４１，Ｂ４２，Ｃ４３のいずれかから送信された秘密鍵ＳＫ＝（ｐ１，ｐ２，ｄ）、公開鍵ＰＫ＝（ｎ，ｅ）と、発行識別子情報ＩＤＩを受信する。

【００８４】

秘密鍵格納部４５ｉ３は、秘密鍵ＳＫ＝（ｐ１，ｐ２，ｄ）を格納する。

公開鍵証明書格納部４５ｉ４は、公開鍵証明書Ｃｅｒｔを格納する。

＜端末装置４５ｉの動作＞

以下に端末装置４５ｉの動作を示す。ここでは、鍵発行サーバＡ４１に鍵発行を依頼する場合の動作を示している。図１４にこの動作のフローチャートを示す。

【００８５】

ステップＳ６０１：送信部４５ｉ１は、鍵発行依頼情報を鍵発行サーバＡ４１へ送信する。

ステップＳ６０２：受信部４５ｉ２は、鍵発行サーバＡ４１より送信された秘密鍵ＳＫ＝（ｐ１，ｐ２，ｄ）、公開鍵証明書Ｃｅｒｔを受信する。

ステップＳ６０３：秘密鍵格納部４５ｉ３は、秘密鍵ＳＫ＝（ｐ１，ｐ２，ｄ）を格納する。

【００８６】

ステップＳ６０４：公開鍵証明書格納部４５ｉ４は、公開鍵証明書Ｃｅｒｔを格納し、終了する。

＜鍵発行システム４の動作＞

以下に鍵発行システム４の動作を示す。以下では、鍵発行サーバＡ４１が端末装置４５ｉに鍵を発行するときの動作を示す。端末装置４５ｉは、まず、鍵発行依頼情報を鍵発行サーバＡ４１へ送信する。鍵発行サーバＡ４１は、鍵発行依頼情報を受信した後、発行識

別子情報ＩＤＩを作成する。その後、鍵発行サーバＡ４１は秘密鍵ＳＫ＝（ｐ１，ｐ２、ｄ）、公開鍵証明書ＰＫ＝（ｎ，ｅ）を生成する。さらに、鍵発行サーバＡ４１は、公開鍵ＰＫ＝（ｎ，ｅ）と発行識別子情報ＩＤＩを証明書発行サーバ４４へ送信する。証明書発行サーバ４４は、公開鍵ＰＫに対応する秘密鍵ＳＫに含まれる素数ｐ１、ｐ２が発行識別子情報ＩＤＩを用いて生成されているかを判定する。証明書発行サーバ４４は、判定結果が肯定的な場合に、公開鍵ＰＫに対する公開鍵証明書Ｃｅｒｔを生成し、公開鍵証明書Ｃｅｒｔを鍵発行サーバＡ４１へ送信する。鍵発行サーバＡ４１は、秘密鍵ＳＫ＝（ｐ１，ｐ２，ｄ）と公開鍵証明書Ｃｅｒｔを端末装置４５ｉへ送信する。端末装置４５ｉは、秘密鍵ＳＫ、公開鍵証明書Ｃｅｒｔを格納し、システムを終了する。

【００８７】

＜実施の形態４の効果＞

実施の形態２と同様の理由で、鍵発行サーバは各端末装置に異なる秘密鍵を発行できる。また、発行識別子情報ＩＤＩに鍵発行サーバの識別子を含んでいるため、各鍵発行サーバごとに異なる秘密鍵を発行できることが証明できる。

証明書発行サーバは、鍵発行サーバが正しく発行識別子情報ＩＤＩを用いて生成しているかを確認することができる。なぜなら、秘密鍵である素数ｐ１、ｐ２はそれぞれ、素数ｑ１、ｑ２、乱数Ｒ１’、Ｒ２’、発行識別子情報ＩＤＩを用いて、ｐ１＝２×ｑ１×ＩＤＩ×Ｒ１’＋１、ｐ２＝２×ｑ２×ＩＤＩ×Ｒ２’＋１を満たすため、

ｎ＝ｐ１×ｐ２＝（２×ｑ１×ＩＤＩ×Ｒ１’＋１）×（２×ｑ２×ＩＤＩ×Ｒ２’＋１）

＝４×ｑ１×ｑ２×Ｒ１’×Ｒ２’×ＩＤＩ＾２＋２×ｑ１×ＩＤＩ×Ｒ１’＋２×ｑ２×ＩＤＩ×Ｒ２’＋１

＝ＩＤＩ×（４×ｑ１×ｑ２×Ｒ１’×Ｒ２’×ＩＤＩ＋２×ｑ１×Ｒ１’＋２×ｑ２×Ｒ２’）＋１

となる。そのため、ｎ－１はＩＤＩで割り切れるため、ｎ－１がＩＤＩで割り切れることを確認することで、素数ｐ１、ｐ２が正しく発行識別子情報ＩＤＩを用いて生成しているかを確認することができる。

【００８８】

なお、以下の確認方法により、不正を働いた端末の情報を得ることができる。不正を働いた端末の秘密鍵ｐ１，ｐ２が判明したとする。また、不正の追跡者は、発行識別子情報と端末の対応表と持っているとする。ｐ１－１，ｐ２－１は共に発行識別子情報ＩＤＩで割り切れる。そのため、ＧＣＤ（ｐ１－１，ｐ２－１）は発行識別子情報で割り切れる。したがって、ＧＣＤ（ｐ１－１，ｐ２－１）の素因数を調べることにより、不正の追跡者は、取りうる発行識別子情報を限定でき、発行識別子情報を知る、すなわち、端末を特定するための助けとなる。

【００８９】

（変形例）

上記に説明した実施の形態は、本発明の実施の一例であり、本発明はこの実施の形態に何ら限定されるものではなく、その旨を逸脱しない範囲において種々なる態様で実施し得るものである。例えば、以下のような場合も本発明に含まれる。

（１）先にも述べたが、実施の形態４における、生成する秘密鍵である素数のビットサイズは５１２に限らない。１０２４であっても、２０４８であってもよい。また、素数情報生成部で生成する素数も同様に２５６ビットに限らない。

【００９０】

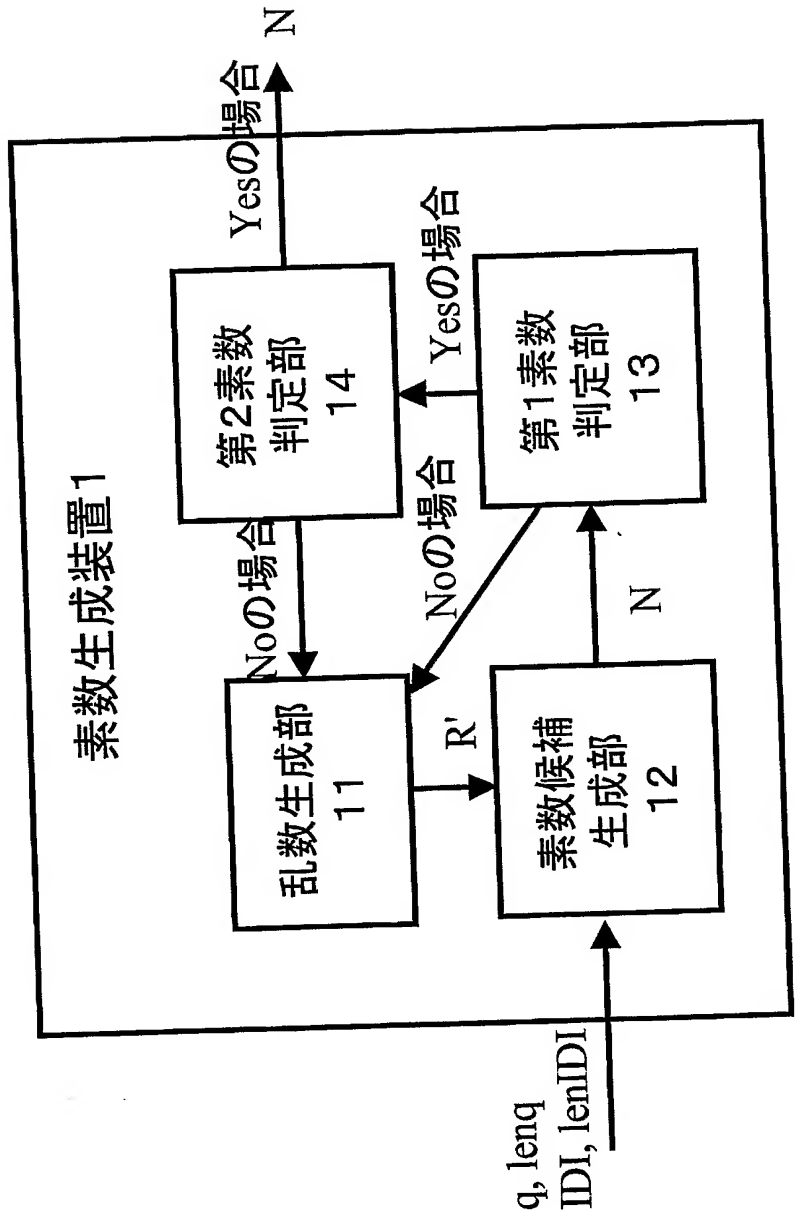
（２）実施の形態１、２または３の素数生成装置を素数生成手段として用いて、整数ｌｅｎと発行識別子情報ＩＤＩを入力とし、ｌｅｎビットの素数を出力する素数生成装置としてもよい。また、実施の形態４の素数情報生成部で使用する素数生成方法は、実施の形態１、２または３の素数生成装置であってもよい。

（３）素数に発行識別子情報を含ませる方法は、実施の形態に限らない。例えば、下位ｌｅｎＩＤＩビットがＩＤＩである素数を生成・発行するとしてもよい。

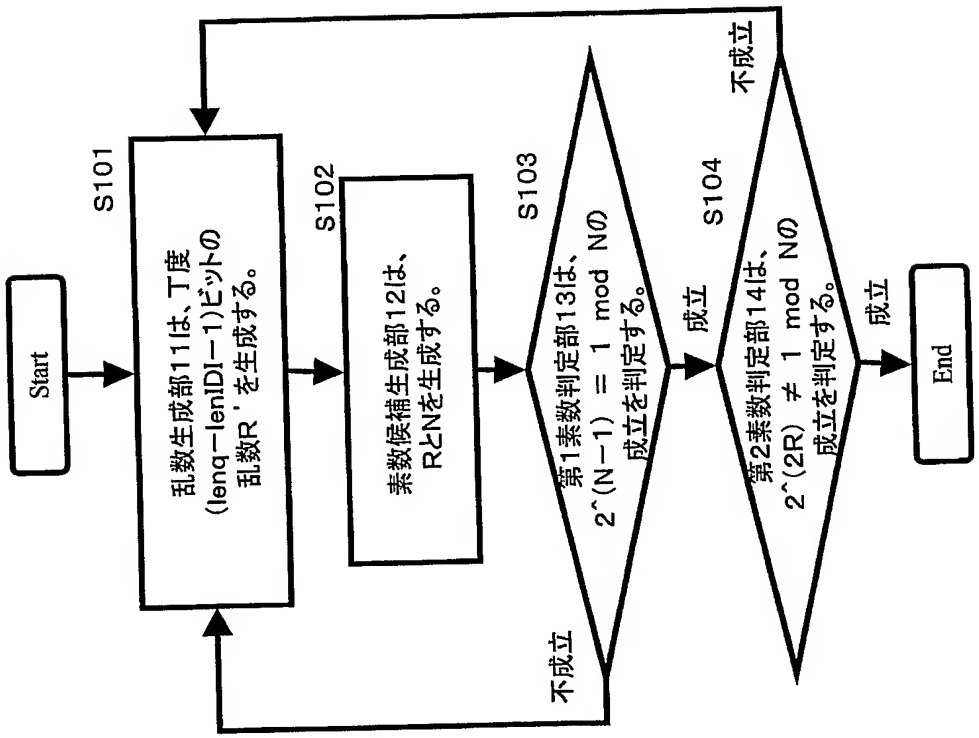
【００９１】
（４）鍵発行サーバは３台以外の何台であってもよい。
【産業上の利用可能性】
【００９２】
これらの構成によると、複数回素数生成を行っても、素数が一致しないことを比較することなく、証明できる素数生成を実現できる。
【図面の簡単な説明】
【００９３】
【図１】本発明に係る１個の実施の形態としての素数生成装置１の構成を示すブロック図
【図２】素数生成装置１の動作を示すフローチャート
【図３】本発明に係る１個の実施の形態としての素数生成装置２の構成を示すブロック図
【図４】素数生成装置２の動作を示すフローチャート
【図５】本発明に係る１個の実施の形態としての素数生成装置３の構成を示すブロック図
【図６】素数生成装置３の動作を示すフローチャート
【図７】本発明に係る１個の実施の形態としての鍵発行システム４の構成を示すブロック図
【図８】鍵発行サーバＡ４１の構成を示す図
【図９】素数生成部４１０５の構成を示す図
【図１０】鍵発行サーバＡ４１の動作を示すフローチャート
【図１１】証明書発行サーバ４４の構成を示す図
【図１２】証明書発行サーバ４４の動作を示すフローチャート
【図１３】端末装置４５ｉの構成を示す図
【図１４】端末装置４５ｉの動作を示すフローチャート
【符号の説明】
【００９４】
１、２、３　素数生成装置
１１、２２、３２　乱数生成部
１２、２３、３３　素数候補生成部
１３　第１素数判定部
１４　第２素数判定部
２１　素数シード生成部
３１　識別子素数生成部
４　鍵発行システム
４１　鍵発行サーバＡ
４１０１、４４１、４５ｉ１　送信部
４１０２、４４２、４５ｉ２　受信部
４１０３　識別子生成部
４１０４　識別子格納部
４１０５　素数生成部
４１０５１　第１の素数生成部
４１０５２　第２の素数生成部
４１０６　秘密鍵判定部
４１０７　鍵生成部
４１０８、４４３、４５ｉ３　秘密鍵格納部
４１０９　公開鍵格納部
４１１０、４５ｉ４　公開鍵証明書格納部
４２　鍵発行サーバＢ

４３　鍵発行サーバＣ
４４　証明書発行サーバ
４４４　発行公開鍵確認部
４４５　発行公開鍵格納部
４４６　公開鍵証明書生成部
４４７　公開鍵証明書格納部
４５ｉ（ｉ＝１～ｎ）　端末装置

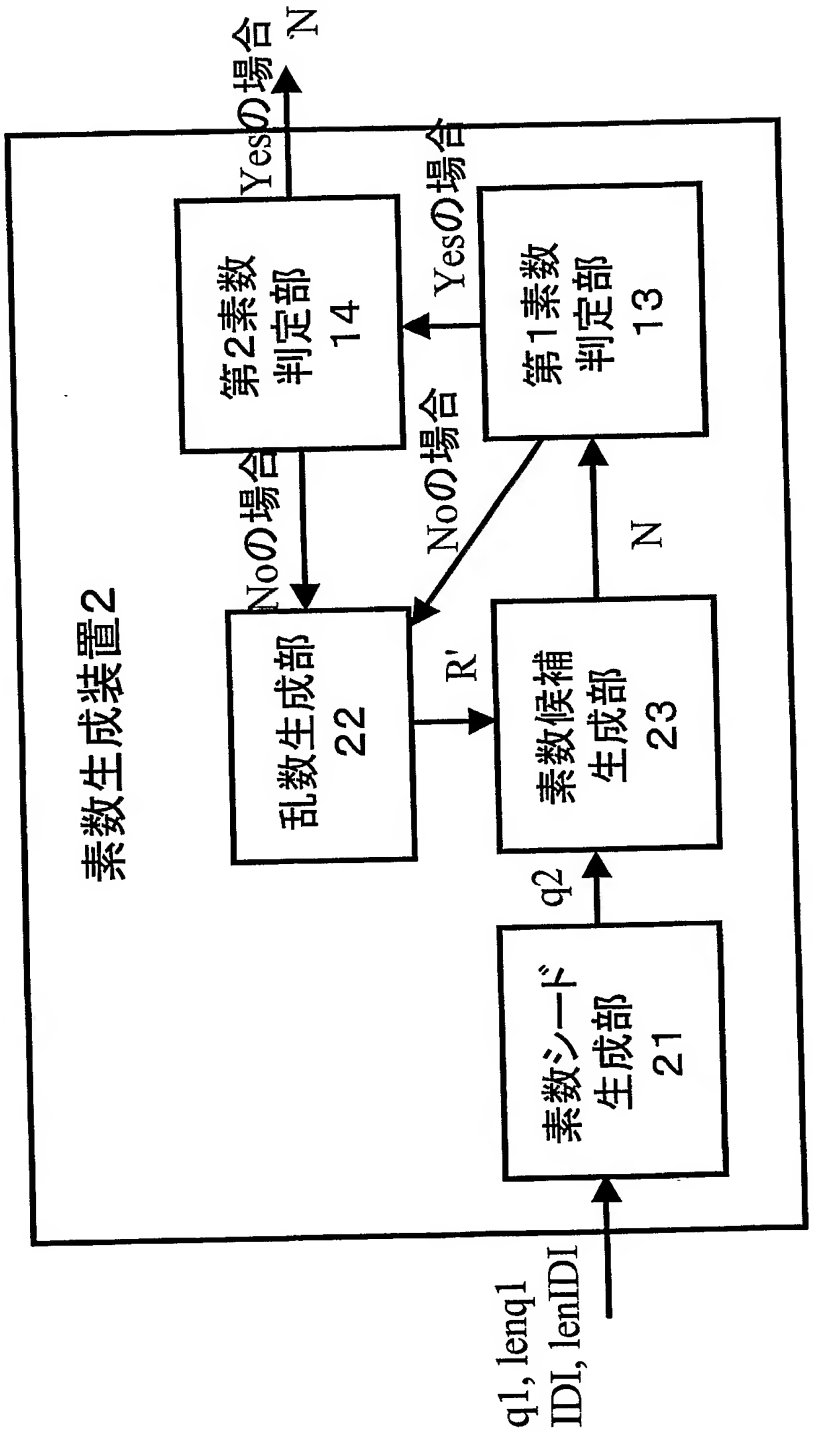
【書類名】図面
【図１】


素数生成装置1
乱数生成部
11
R'
素数候補
生成部
12
第1素数
判定部
13
第2素数
判定部
14
Noの場合
Yesの場合
Noの場合
Yesの場合
N
N
q, lenq
IDI, lenIDI

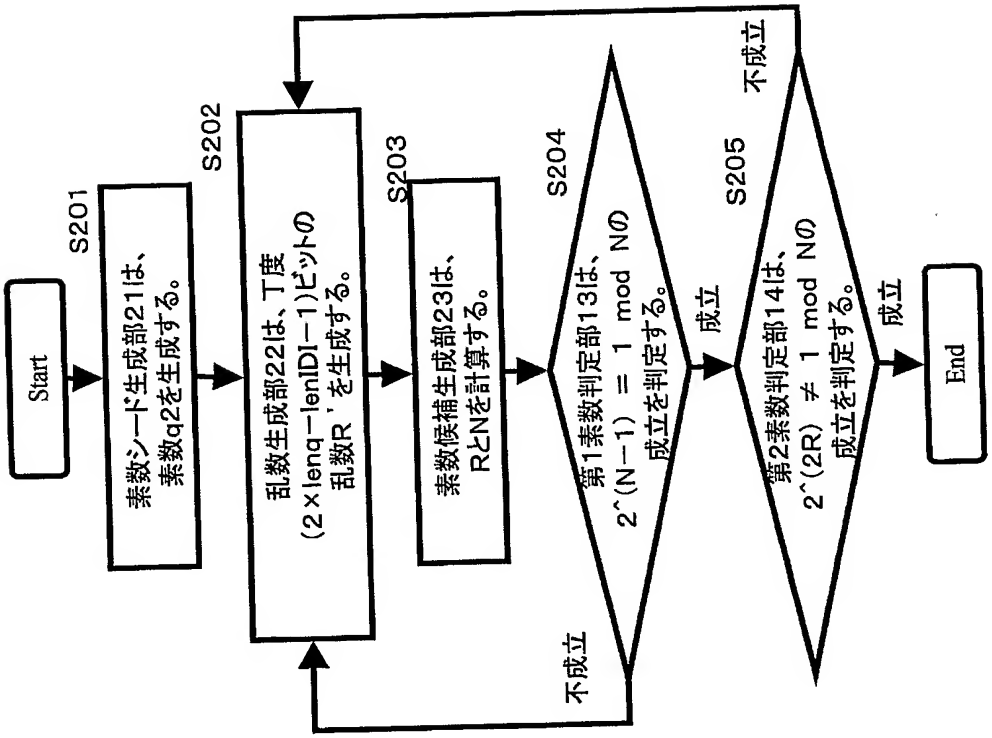
【図２】


Start
S101
乱数生成部11は、T度
(lenq−lenIDI−1)ビットの
乱数R'を生成する。
S102
素数候補生成部12は、
RとNを生成する。
S103
第1素数判定部13は、
2^(N−1) ＝ 1 mod Nの
成立を判定する。
不成立
成立
S104
第2素数判定部14は、
2^(2R) ≠ 1 mod Nの
成立を判定する。
不成立
成立
End

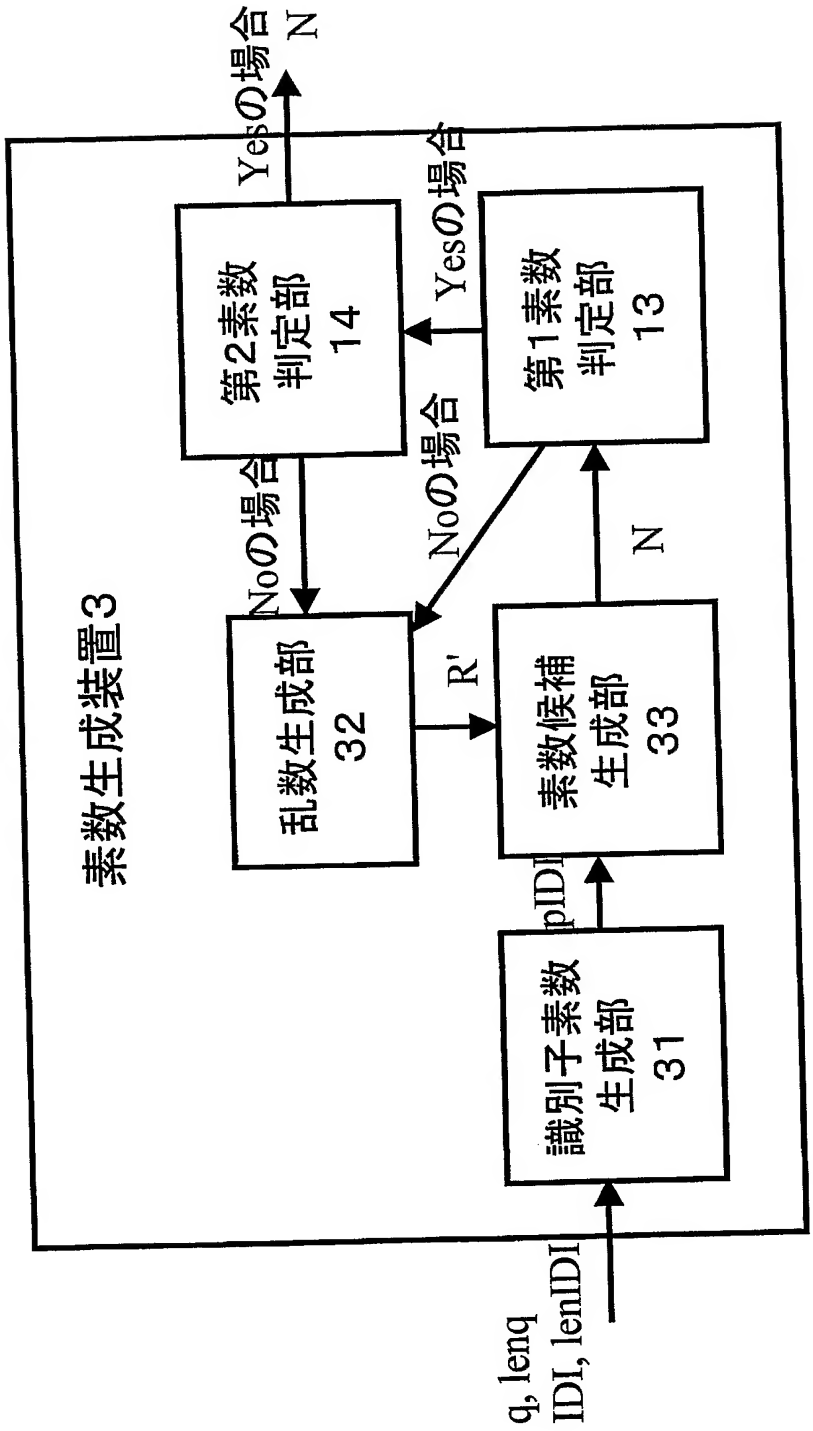
【図３】


素数生成装置2
素数シード生成部 21
乱数生成部 22
素数候補生成部 23
第1素数判定部 13
第2素数判定部 14
q1, lenq1
IDI, lenIDI
q2
R'
N
Noの場合
Yesの場合
N
Noの場合
Yesの場合

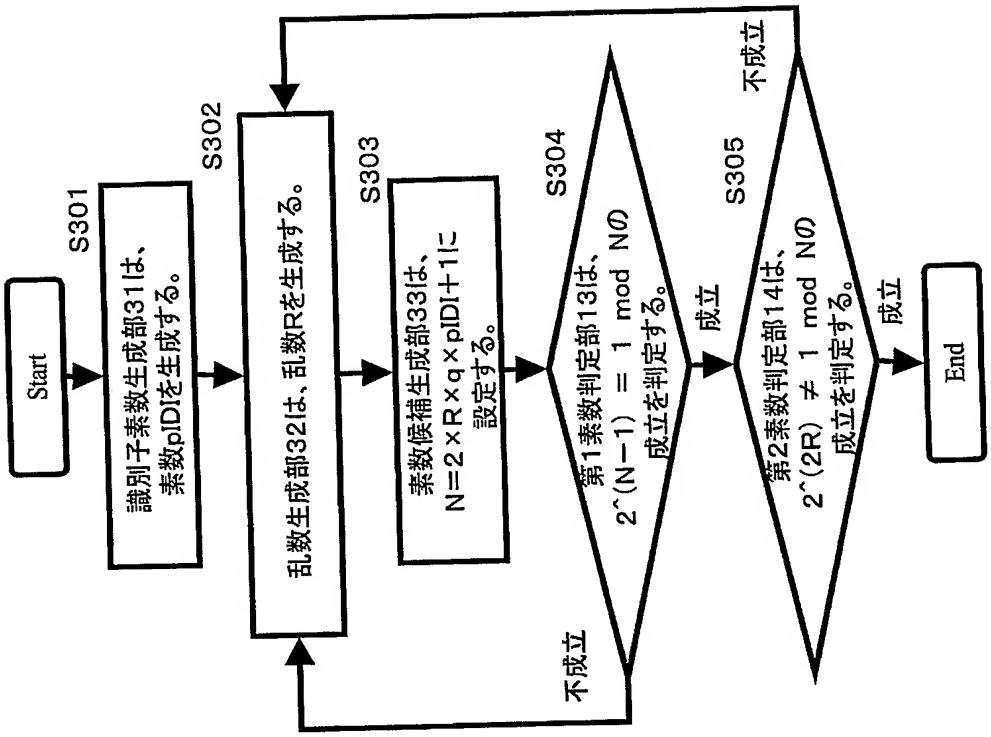
【図４】


Start
S201
素数シード生成部21は、
素数q2を生成する。
S202
乱数生成部22は、下度
(2×lenq−lenIDI−1)ビットの
乱数R'を生成する。
S203
素数候補生成部23は、
RとNを計算する。
S204
第1素数判定部13は、
2^(N−1) ＝ 1 mod N0
成立を判定する。
不成立
成立
S205
第2素数判定部14は、
2^(2R) ≠ 1 mod N0
成立を判定する。
不成立
成立
End

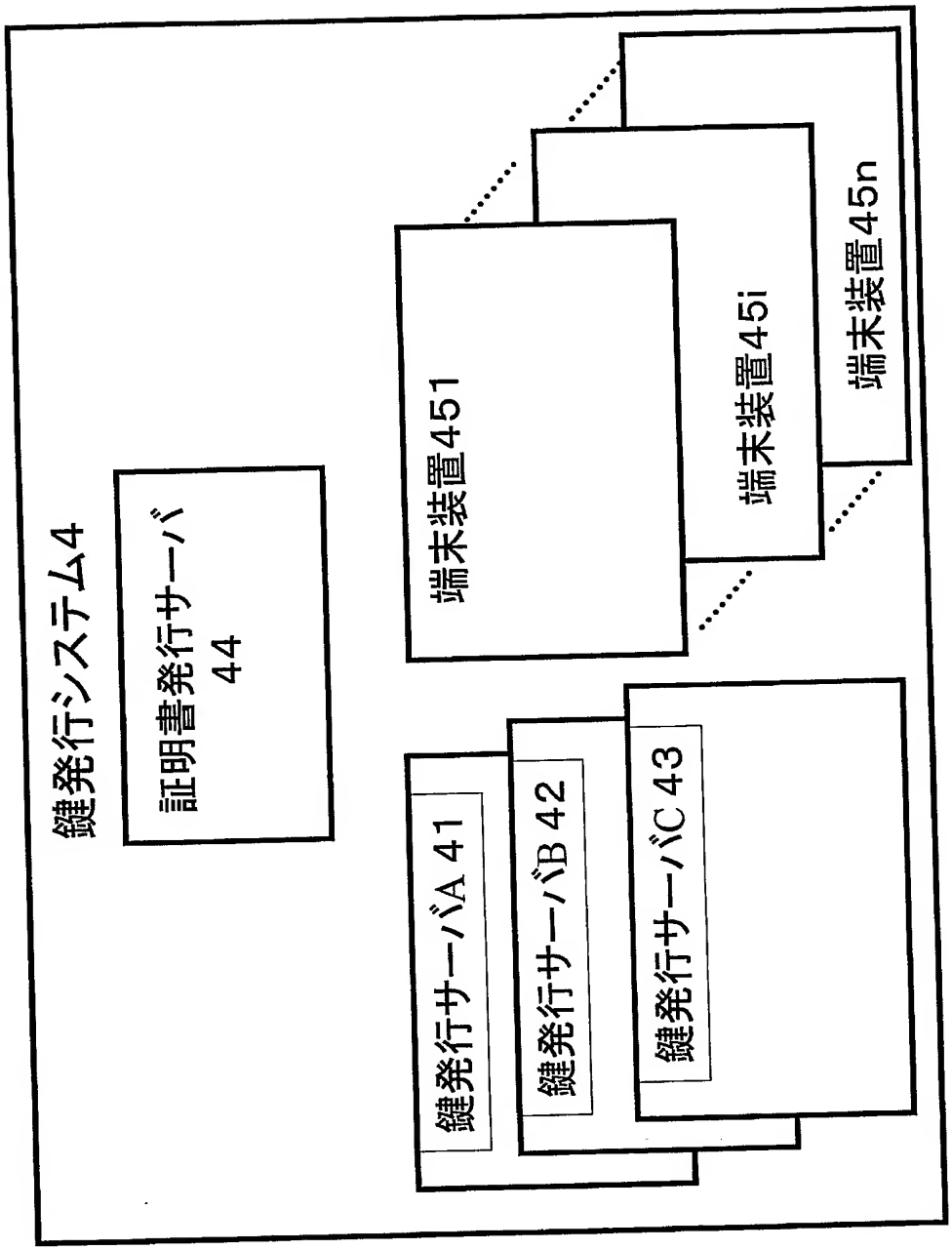
【図５】


素数生成装置3
識別子素数生成部 31
乱数生成部 32
素数候補生成部 33
第1素数判定部 13
第2素数判定部 14
q, lenq
IDI, lenIDI
pIDI
R'
Noの場合
Yesの場合
N

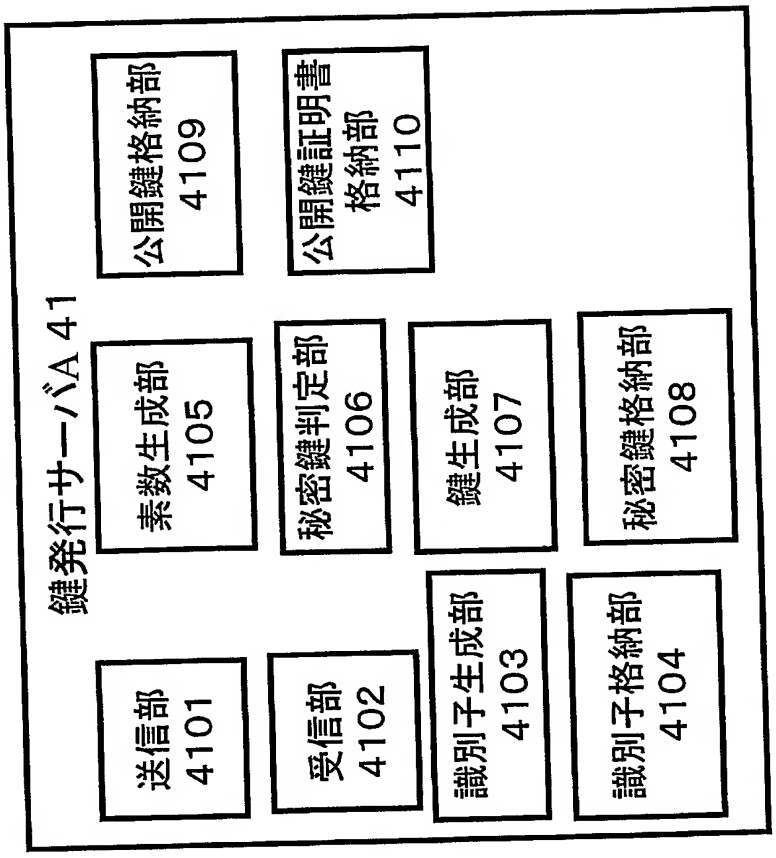
【図６】


Start
S301
識別子素数生成部31は、
素数pIDiを生成する。
S302
乱数生成部32は、乱数Rを生成する。
S303
素数候補生成部33は、
N=2×R×q×pIDi+1に
設定する。
S304
第1素数判定部13は、
2^(N−1) = 1 mod N0
成立を判定する。
不成立
成立
S305
第2素数判定部14は、
2^(2R) ≠ 1 mod N0
成立を判定する。
不成立
成立
End

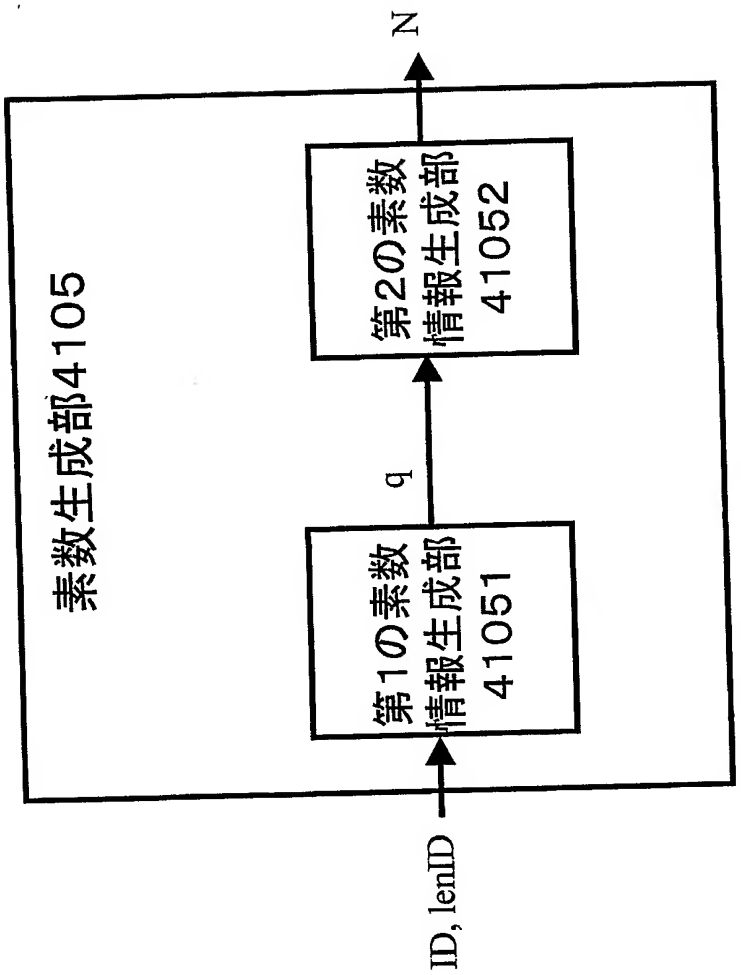
【図７】


鍵発行システム4
証明書発行サーバ
44
鍵発行サーバA 41
鍵発行サーバB 42
鍵発行サーバC 43
端末装置451
端末装置45i
端末装置45n

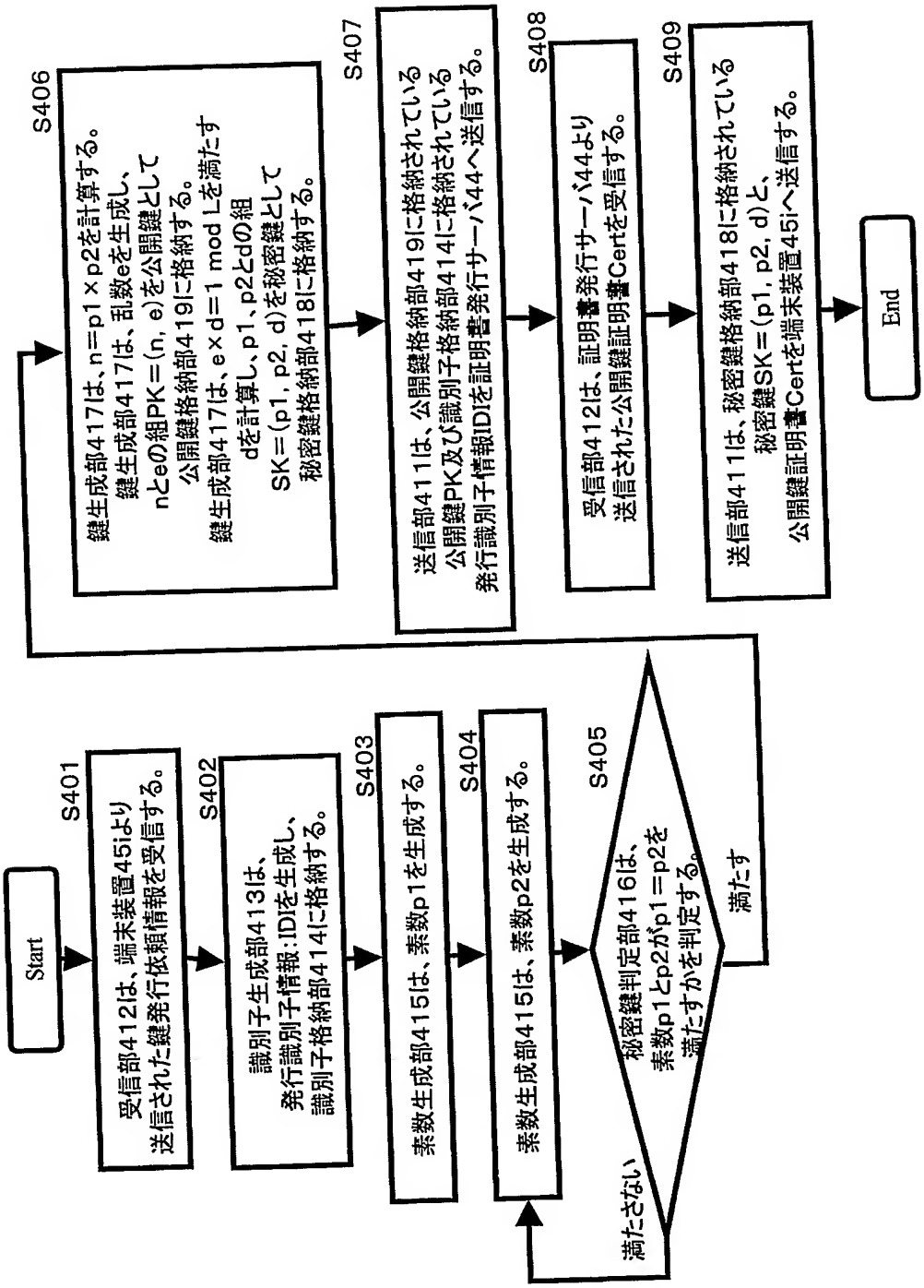
【図８】


鍵発行サーバA 41
送信部 4101
受信部 4102
識別子生成部 4103
識別子格納部 4104
素数生成部 4105
秘密鍵判定部 4106
鍵生成部 4107
秘密鍵格納部 4108
公開鍵格納部 4109
公開鍵証明書格納部 4110

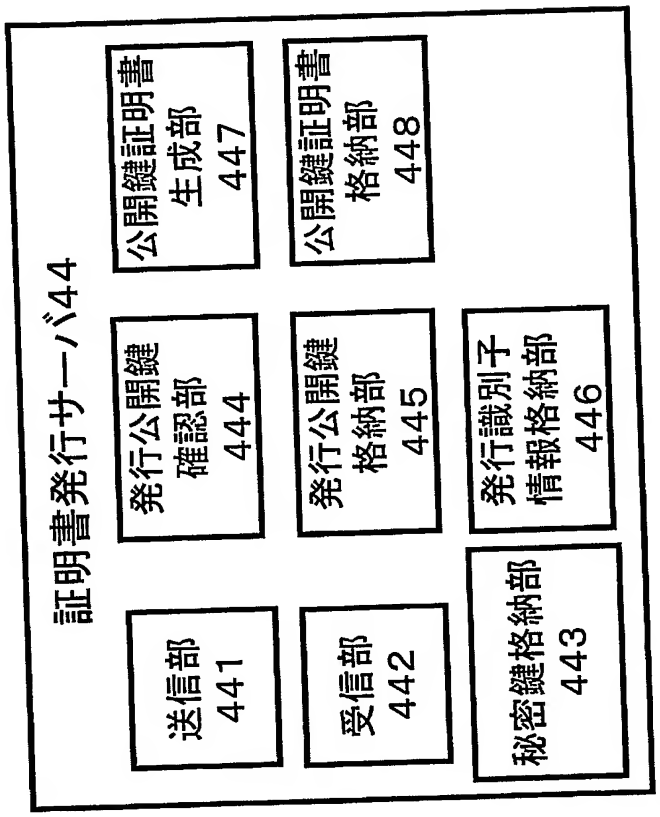
【図９】



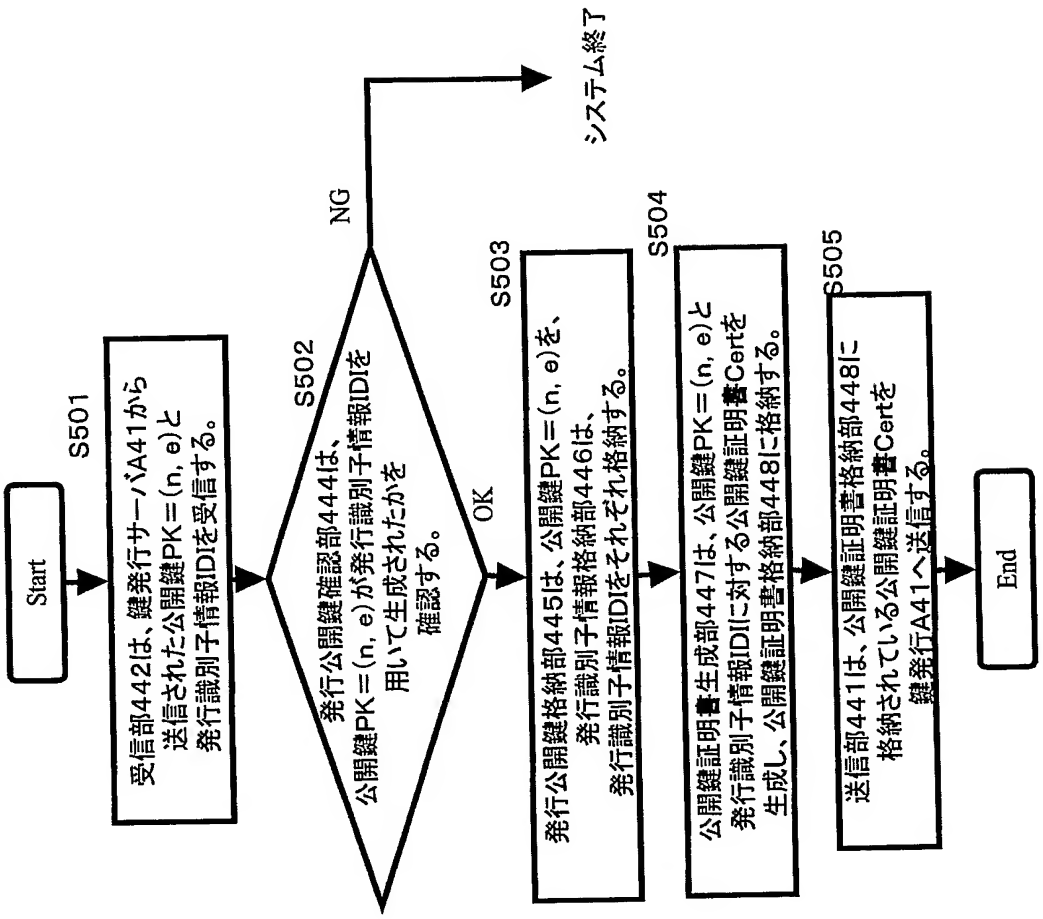
【図１０】


Start
S401
受信部412は、端末装置45iより
送信された鍵発行依頼情報を受信する。
S402
識別子生成部413は、
発行識別子情報:IDiを生成し、
識別子格納部414に格納する。
S403
素数生成部415は、素数p1を生成する。
S404
素数生成部415は、素数p2を生成する。
S405
秘密鍵判定部416は、
素数p1とp2がp1＝p2を
満たすかを判定する。
満たさない
満たす
S406
鍵生成部417は、n=p1×p2を計算する。
鍵生成部417は、乱数eを生成し、
nとeの組PK＝(n, e)を公開鍵として
公開鍵格納部419に格納する。
鍵生成部417は、e×d=1 mod Lを満たす
dを計算L、p1、p2とdの組
SK＝(p1, p2, d)を秘密鍵として
秘密鍵格納部418に格納する。
S407
送信部411は、公開鍵格納部419に格納されている
公開鍵PK及び識別子格納部414に格納されている
発行識別子情報IDiを証明書発行サーバ44へ送信する。
S408
受信部412は、証明書発行サーバ44より
送信された公開鍵証明書Certを受信する。
S409
送信部411は、秘密鍵格納部418に格納されている
秘密鍵SK＝(p1, p2, d)と、
公開鍵証明書Certを端末装置45iへ送信する。
End

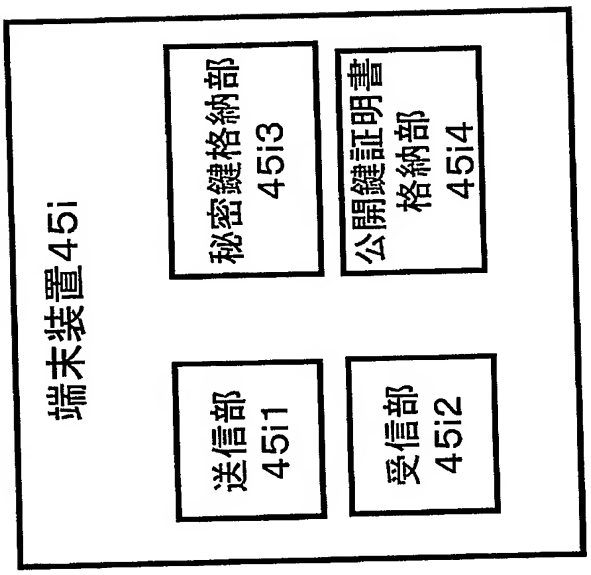
【図１１】


証明書発行サーバ44
送信部
441
受信部
442
秘密鍵格納部
443
発行公開鍵
確認部
444
発行公開鍵
格納部
445
発行識別子
情報格納部
446
公開鍵証明書
生成部
447
公開鍵証明書
格納部
448

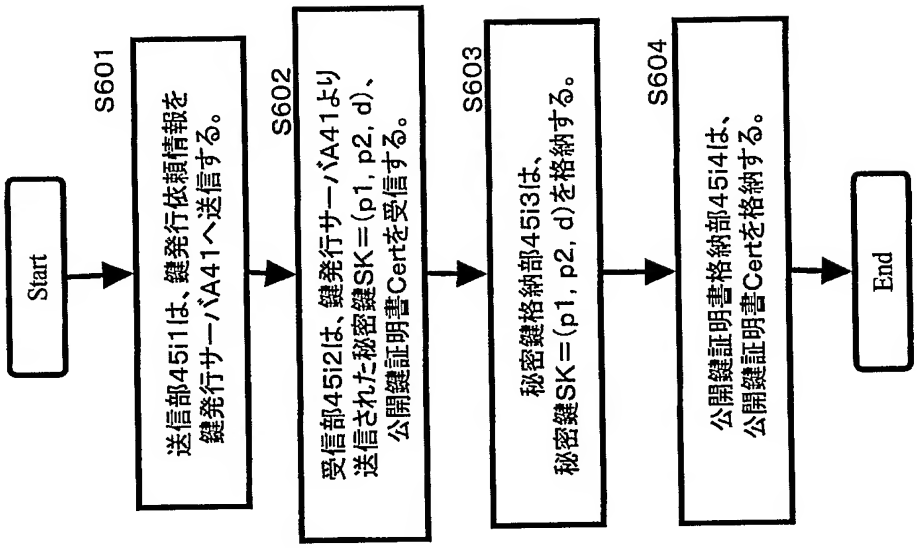
【図１２】


Start
S501
受信部442は、鍵発行サーバA41から
送信された公開鍵PK＝(n, e)と
発行識別子情報IDを受信する。
S502
発行公開鍵確認部444は、
公開鍵PK＝(n, e)が発行識別子情報IDを
用いて生成されたかを
確認する。
NG
システム終了
OK
S503
発行公開鍵格納部445は、公開鍵PK＝(n, e)を、
発行識別子情報格納部446は、
発行識別子情報IDをそれぞれ格納する。
S504
公開鍵証明書生成部447は、公開鍵PK＝(n, e)と
発行識別子情報IDに対する公開鍵証明書Certを
生成し、公開鍵証明書格納部448に格納する。
S505
送信部441は、公開鍵証明書格納部448に
格納されている公開鍵証明書Certを
鍵発行A41へ送信する。
End

【図１３】



【図１４】


Start
S601
送信部451は、鍵発行依頼情報を鍵発行サーバA41へ送信する。
S602
受信部452は、鍵発行サーバA41より送信された秘密鍵SK＝(p1, p2, d)、公開鍵証明書Certを受信する。
S603
秘密鍵格納部453は、秘密鍵SK＝(p1, p2, d)を格納する。
S604
公開鍵証明書格納部454は、公開鍵証明書Certを格納する。
End

【書類名】要約書
【要約】
【課題】　従来技術では、複数回素数生成を行ったときに素数が一致する可能性があり、それにより、暗号の安全性を著しく低下させるという課題がある。また、生成した素数をチェックすることは、素数が増加すると困難になる。
【解決手段】　鍵発行サーバは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成部と、を備え、前記端末装置は、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵を格納する公開鍵格納部と、を備える。素数に発行識別子を埋め込むことにより、発行識別子ごとに異なる素数を生成できる。
【選択図】　図４

特願２００３－４３３９０３

出　願　人　履　歴　情　報

識別番号　［０００００５８２１］

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社